

Attachment E

Terms and Obligations Related to Transfer of Clinical Preventive Health Services from SAMHD to UHS

<u>Section 1 – Scope of Transition</u>	2
<u>Section 2 – Organizational Structure and Culture</u>	2
<u>Section 3 – Clinical Operations and Medical Providers</u>	3
<u>Section 4 – Facilities</u>	4
<u>Section 5 – Information Systems</u>	6
<u>Section 6 – Human Resources</u>	8
<u>Section 7 – Funding Plan</u>	11
<u>Section 8 – Grants/Contracts and Billing</u>	12
<u>Section 9 – Ancillary Services</u>	13
<u>Section 10 – Health Promotion/Preventive Health Programs</u>	13
<u>Section 11 – Utilization of UHS Staff for Public Health Events/Public Health Emergencies</u>	15
<u>Section 12 – Assuring Quality of Transitioned Services</u>	17
<u>Section 13 – Joint Planning and Operations Council</u>	18
<u>Section 14 – Governing Law and Severability</u>	19
Exhibit A: Medical Staff and Prevention Program Organization	21
Exhibit B: Clinical Preventive Health Service Sites	22
Exhibit C: CoSA Administrative Directives Governing IT Use	23
Exhibit D: UHS Benefits Summary	51
Exhibit E: Positions and Other Expense Items	56
Exhibit F: Summary of SAMHD Grants for Services Transitioning to UHS	58

Section 1 – Scope of Transition

The San Antonio Metropolitan Health District (SAMHD) will transfer operation of clinical preventive health services, including prenatal services, family planning services, well-child exams, senior health services, breast and cervical cancer screenings, and refugee health screening services, to the University Health System (UHS) on February 4, 2008. This transfer will include staff (public health nurses, public health aides, administrative /office assistants, medical providers, etc.) and the immediate use of 9 SAMHD/City of San Antonio (City) clinic facilities via lease agreement. SAMHD and UHS will each independently execute agreements with the San Antonio Housing Authority (“SAHA”) to secure the use of, and provide services in, the SAHA-owned Ricardo Salinas clinic facility.

Section 2 – Organizational Structure and Culture

Organizational Structure and Services

- a) Initially, transferred SAMHD staff will be maintained in one organizational division within the Health System’s Ambulatory Services division. Direct supervision of transferred nursing staff will be through the position of Nursing Program Manager. The Nursing Program Manager will report to the Vice President/UCCH & Community Health Services. The organizational placement of providers and staff within UHS is shown in Exhibit A. Staff in support positions such as accountants, custodians, IT specialists, etc. will become part of existing UHS Ambulatory Services support services divisions.
- b) The Joint Planning and Operations Council (JPOC) will be the primary vehicle for collaborative planning between the SAMHD and UHS. This body will develop plans, identify resources, and seek approval from both the City of San Antonio and UHS governance and management to assure that the public health needs of Bexar County residents are met.

Organizational Culture for Prevention

- c) Long-term objectives of this transfer of services are to strengthen the focus on health, wellness, and prevention within the City and County and expand preventive health services, health education, and community-based outreach within UHS.
- d) In addition to continuing operations of current SAMHD sites, UHS proposes to assign a few key, experienced public health nurses to roles within the UHS primary care clinic sites in order to identify opportunities for expanded prevention, health education, and community-based outreach.
- e) The UHS ambulatory services division will incorporate public health core values into its evolving mission and values statements.

Section 3 – Clinical Operations and Medical Providers

Clinic Operations

- a) UHS will ensure that adequate resources are committed to maintain the same or higher level of productivity at all clinic locations to include, but not be limited to staffing, supplies, and support services. To maintain transparency of the service transition to clients in the community, there will be adequate mechanisms and protocols in place to enable clinic operations to function by February 4, 2008.
- b) The Health System shall maintain the current SAMHD service locations and existing hours of operation from February 4, 2008 through December 31, 2008. UHS agrees that the number of hours of service provided at any site will not be reduced during this timeframe. Should UHS determine that the clinic schedule should be adjusted to provide better patient service the proposed change will be addressed through the JPOC. Upon agreement by the JPOC, and upon proper public notice the change in hours shall be instituted. It is understood that the clinics will follow the UHS holiday schedule. During this period, the Health System will analyze and evaluate potential efficiencies and improvements for incorporation into the 2009 tax rate proposal and operating budget. Any proposed changes affecting service delivery at the preventive health clinics will be shared through the JPOC to support continued coordination of services.
- c) As services of the University Health System, these operations will be subject to Joint Commission standards effective February 4, 2008.
- d) New patient medical records will be established by University Health System. Prior to February 4, 2008, SAMHD staff will facilitate continuity of care by providing UHS with copies of medical records of SAMHD patients who have an appointment in a UHS medical facility. SAMHD will then close and store all medical records for patients served in SAMHD preventive health clinics. After February 4, 2008, UHS may obtain a copy of a patient record by submitting a request to SAMHD that is signed by the patient or the patient's parent/guardian or by providing evidence that the patient has an appointment in a UHS facility. SAMHD patient records will be archived for the period(s) required by applicable state and federal law and then destroyed.

Medical Providers

- e) Transitioning clinical preventive services are currently provided by:
- six full-time nurse-practitioners;
 - one part-time nurse practitioner;
 - one full-time physician; and,
 - four part-time physicians.
- f) UHS currently has contracts with the UTHSCSA Departments of Obstetrics and Gynecology to provide medical staffing for prenatal services at SAMHD sites and may explore cooperative arrangements with additional clinical departments in the future. UTHSCSA Family Practice is currently staffing clinics and will be allowed to continue as they do now.

g) Current SAMHD providers who are providing services at the clinics listed in Exhibit B and that are affected by the transfer of services will be supervised and evaluated by a new prevention division of Community Medicine Associates (CMA) and/or an appropriate UTHSCSA Department.

h) CMA and UTHSCSA will execute an agreement to define the working relationship in the affected clinics for UT and CMA providers.

i) The new prevention division within CMA will have a representative on the JPOC and will be involved with operational planning for prevention and community health activities in partnership with SAMHD.

j) Current SAMHD providers who are providing services in clinics listed in Exhibit B and affected by the transfer of services will be credentialed by the University Health System.

Section 4 – Facilities

a) The City of San Antonio will allocate space in ten (10) SAMHD locations for UHS to provide clinical services.

Six (6) of these facilities are owned by the City of San Antonio and occupied solely by SAMHD:

- Eastside Branch (210 N. Rio Grande)
- Kenwood Clinic (302 Dora),
- Old Highway 90 Clinic (911 Old Highway 90 West),
- Pecan Valley Clinic (802 Pecan Valley),
- South Flores Clinic (7902 S. Flores), and
- Zarzamora Clinic (4503 S. Zarzamora).

SAMHD will transfer all functions in the Old Highway 90 and South Flores clinics to UHS. UHS shall be the sole occupant of these two (2) clinics upon transfer of the functions set out herein.

SAMHD will continue to provide services, separate and apart from those transferred to UHS in the remainder of the clinics listed above (Eastside, Kenwood, Pecan Valley, and Zarzamora).

Three (3) of these facilities are owned by the City of San Antonio and occupied by multiple CoSA departments including SAMHD:

- Bob Ross Multi-service Senior and Resource Center (2219 Babcock),
- Frank Garrett Community Family Resource and Learning Center (1226 NW 18th St.), and
- Naco-Perrin Clinic (4020 Naco-Perrin)

Space can be made available in one (1) other City facility that is not currently providing SAMHD clinical preventive services if UHS wishes to expand services into this location:

- Southwest Branch (9011 Poteet-Jourdanton Freeway)

The City is currently leasing 9,522 square feet of space in Southwest Branch Clinic to CentroMed. This lease may be terminated upon 120 days written notice to the lessee and made available to UHS, if required. (See Exhibit B).

From February 4, 2008 through December 31, 2008 the space, as outlined in Exhibit B, will be provided to the Health System via a comprehensive lease agreement which will include a floor plan of each facility and the square footage to be occupied solely by the Health System along with space to be shared with other programs.

b) Space will also be allocated in one (1) facility owned by the San Antonio Housing Authority (SAHA):

- Salinas Clinic (630 Gen. McMullen)

This space, as identified in Exhibit B, will be made available to the Health System via Lease Agreement between SAHA and UHS which will provide that the Health System will provide clinical services to SAHA residents without charge in lieu of paying rent for the facility. SAMHD will assist UHS in establishing an agreement with SAHA for 2008. Any agreement after 2008 will be the sole responsibility of UHS. It is anticipated that SAMHD and UTHSCSA Dental will also have leases at this facility and will provide clinical services to SAHA residents subject to their individual leases.

c) The City will pay UHS to operate said clinical preventive health facilities from February 4, 2008- December 31, 2008. UHS will be responsible for the cost of any additional equipment, services, or renovations that are procured for the leased space.

d) The City agrees that if UHS wishes to continue to provide services at the following locations after December 31, 2008, City will provide UHS with long term rent-free lease space in each of the following facilities on January 1, 2009.

- Bob Ross Multi-service Senior and Resource Center (2219 Babcock),
- Frank Garrett Community Family Resource and Learning Center (1226 NW 18th St.), and
- Naco-Perrin Clinic (4020 Naco-Perrin)

e) The City agrees that it will transfer, per separate written agreement, the following facilities to UHS on January 1, 2009: Eastside, Kenwood, Old Highway 90, Pecan Valley, South Flores and Zarzamora Clinics. This transfer will be made pursuant to Texas Local Government Code §253.011 and is contingent upon completion of title investigation of each property, presentation and approval by the City of San Antonio Planning Commission, approval by City Council and associated due diligence. If, in the event that the transfer to UHS of any or all of the locations within this section is not approved by the City of San Antonio Planning Commission and/or City Council, the City agrees that if UHS wishes to continue to provide services at these locations after December 31, 2008, City will provide UHS with long term rent-free lease space at each of

the facilities in which UHS has operations or occupancy on January 1, 2009 via City Council-approved lease agreement.

f) If the transfer of facilities identified in paragraph (e) is approved and in effect on January 1, 2009, UHS will provide SAMHD with rent-free lease space in each of these facilities in which SAMHD has operations or occupancy on January 1, 2009.

g) The provision of light maintenance, housekeeping, landscaping and mowing at these facilities will be the responsibility of the on-site custodial staff included in the transition of services from the SAMHD and UHS. Major facility repairs, HVAC replacement, or maintenance issues will remain the responsibility of the building owner and will be addressed in any and all short term and long term lease agreement(s) and/or transfer of facilities.

h) Current clinic furniture and equipment, to include desks, chairs, business machines, information technology, security and communications equipment at these sites will remain in place for use by the Health System from February 4, 2008- December 31, 2008 and will be included in any and all short term and long lease agreement(s) and/or transfer of facilities. Health System staff and patients will have free access to the parking areas of each facility.

i) From February 4, 2008- December 31, 2008, the City will be responsible for maintaining the current security systems at the facilities including building alarms, equipment alarms (vaccine freezers and refrigerators) and security cameras installed inside and outside of the facilities. Maintenance of this equipment will remain the responsibility of the building owner after January 1, 2009 and will be addressed in any and all lease agreement(s) and/or transfer of facilities.

j) Any alterations, additions or remodeling of the COSA facilities listed in Exhibit B from February 4, 2008- December 31, 2008 will be subject to the written lease agreement between SAMHD/CoSA and UHS and subject to any and all long term lease agreements thereafter.

Section 5 – Information Systems

Infrastructure and Equipment

a) The existing City of San Antonio information technology and support infrastructure will remain intact at the facilities transitioned to the Health System through December 31, 2008.

b) Additional equipment that is needed (hardware, pagers, cell phones, etc.) after February 4, 2008 will be provided by the Health System.

c) Information Technology (IT) equipment and systems such as telephones, computers, cell phones, pagers, printers, fax machines, networks, and similar assets owned by SAMHD will remain at said facilities for use by Health System staff as needed.

d) Health System employees using City communications and technology equipment will comply with City Administrative Directives 7.3, 7.4, 7.5 and 7.6 (attached hereto as Exhibit C) while said equipment is in use, and may have their access to this equipment suspended if these

directives are violated. Said violations may also subject employees to disciplinary action pursuant to established UHS policies and directives.

e) SAMHD and UHS will transition to UHS networks during the period from February 4, 2008- December 31, 2008 at UHS expense if technology performance is severely impacted during this time. It is acknowledged that any significant IT change to a City facility must be approved and coordinated through the Information Technology Services Department of the City of San Antonio.

f) The Health System will be responsible for providing services required by the Texas Department of State Health Services and input into the Texas Wide Integrated Client Encounter System (TWICES) for immunization registry purposes and monitoring of grants. SAMHD will assist UHS in setting up billing capability on TWICES to facilitate payments for services provided under State grant programs. UHS will allow SAMHD to view TWICES data for performance management purposes as outlined in Section 12.

g) UHS will install its data and voice networks into facilities upon determination of how these facilities will be utilized. UHS will work with and coordinate with the City of San Antonio's Information Technology Services Department (ITSD) with regard to the installation of equipment or systems, or the removal of unneeded equipment and access. It is understood that all installations or removals will comply with the comprehensive lease agreement in place between the parties.

System Access

h) As of February 4, 2008, SAP access for staff transitioning to UHS will be disabled. SAMHD and UHS will evaluate the need for UHS staff to retain COSA email, as needed using specific criteria and/or for select personnel.

i) UHS will provide access, as needed, to its applications to include IDX, Sunrise, email and associated training.

j) UHS staff will abide by UHS and SAMHD information technology policies where both systems are accessed. UHS will ensure that all equipment and IT services provided by SAMHD will be used only to conduct clinical preventive health services and will be safeguarded from misuse or theft.

Support

k) Support services (i.e. response to "trouble tickets") from February 4, 2008- December 31, 2008 will continue to be provided by the City of San Antonio for equipment, voice, and network systems. Requests will be submitted through the SAMHD Department Systems Manager.

Data Sharing

- 1) UHS and SAMHD will explore opportunities to share data as permitted by law that better serves the public health of the county.

Section 6 – Human Resources

Date of Service

- a) All employees transitioning from SAMHD to University Health System will have a new start date of employment of February 4, 2008. UHS will recognize employee's relevant professional experience when computing salary and time of service with the City with regard to the accrual of paid time off (as described in Exhibit D attached hereto).

Employee Benefits

- b) All employees transitioning from SAMHD to University Health System will be eligible for benefits including but not limited to: health, dental, life, short and long-term disability, etc. (as described below and in Exhibit D attached hereto):

Health Benefits:

- i) University Health System will waive the waiting period for medical health benefits. The effective date of coverage will be February 4, 2008. All election forms must be submitted by transitioning employees to UHS Human Resources in compliance with UHS requirements for a February effective date. The parties agree and acknowledge that waiting periods tied to "voluntary" health benefits cannot be waived.

Voluntary Benefits:

- 1) University Health System offers a variety of Voluntary Benefits to their employees, with no subsidy from UHS. Some of these benefits are currently provided to City employees with a City subsidy (i.e. Life insurance, Short-term Disability). As such, the parties acknowledge that there may be some gaps in coverage that are out of the control of both UHS and the City. These benefits are described in the attached Exhibit.

Retirement Plans:

- ii) All employees transitioning from SAMHD to University Health System will be eligible to participate in the Pension and 457 Retirement Savings Plan based on the current participation formula. The University Health System Board will waive the one-year waiting period for eligibility and contributions into the Pension and 457 Plan.
- iii) City employees who are vested in TMRS will not lose their contributions or the City's 2-1 match, up to the date of transition, if the account remains active through age 60. Additionally, a City employee who is eligible for retirement may retire prior to transfer to University Health System and still make the transition of employment to UHS.

- 1) City of San Antonio employees who are within six (6) months of vesting or retirement eligibility will transition to UHS on February 4, 2008, while completing their TMRS requirement by separate agreement with the City.

Transfer of Annual Leave

iv) The City of San Antonio will pay out some or all of the value of remaining annual leave balance to the employees prior to their ending employment date. The employee can decide whether to receive payment in increments of 25% (rounded up to the nearest hour). Payment to the employee will be made at their respective City rate of pay. The City of San Antonio will pay University Health System any remainder of the current annual leave balances at the UHS rate of pay. University Health System will accept payment for all leave balances and credit the transferring employee with the leave balance hours accordingly.

Employees will accrue leave at UHS at an accrual rate based on years of service with the City of San Antonio. The accrual rate will begin on the first day of employment.

Leave without Pay

v) University Health System will waive the 90-day waiting period for employees to take Leave Without Pay.

Employee Compensation

c) All employees transitioning to University Health System will be paid in accordance with the Compensation and Benefits plan considering internal equity adjustments if applicable.

Job Descriptions

d) Initially all SAMHD job descriptions will be utilized to ensure a seamless transition and provide University Health System management an opportunity to recommend revisions as deemed appropriate. Qualifications, new functions, etc. will need to be determined and finalized by clinic management.

Staff Orientation

e) All employees transitioning from SAMHD to University Health System will participate in a two-day (four day for clinical staff) orientation to the System. New employees will receive information, material, ID badge, parking permit (if applicable), etc. in preparation for a February 4, 2008 start date.

Transition of City Staff

f) Designated part-time and grant positions and personnel will transfer to University Health System on February 4, 2008.

- Grant employees will transfer to regular full-time status positions at University Health System, and will be eligible for benefits with University Health System.
- Part-time employees will transfer to regular part-time status positions at University Health System, and will be eligible for reduced benefits (based on number of hours budgeted to work) with University Health System.

g) The City will attempt to place all support personnel identified by SAMHD that are not part-time or grant-funded, within alternate City of San Antonio jobs. Employees in this category will have the option to transfer to University Health System or to stay with the City of San Antonio.

h) All full-time, non-grant funded clinical personnel and positions identified by SAMHD, who have been employed by the City for less than 15 years as of February 4, 2008, will transfer to University Health System on February 4, 2008

i) All full-time, non-grant funded clinical personnel and positions identified by SAMHD, who have been employed by the City for more than 15 years as of February 4, 2008 will have the option to transfer to University Health System or stay within the City of San Antonio. Some eligible employees will have the option of retiring from the City. Those employees who retire prior to transfer to UHS may still make the transition of employment to UHS.

j) All City of San Antonio positions associated with the University Health System merger will be eliminated on February 4, 2008 unless the person holding the position is not actively at work on that date (on short-term disability, long-term disability, workers compensation, FMLA). Those positions will be eliminated upon return to work and the personnel will transfer to UHS as outlined above.

k) All vacancies will be transferred to University Health System on February 4, 2008 at the value of the City of San Antonio base salary rate.

Reimbursement of Personnel Costs

l) The City will only reimburse for the term of this Agreement for:

- Salary and social security costs budgeted in the FY 2008 Adopted budget for identified support and clinical positions
- Vacant positions will be funded at the base rate of the City of San Antonio
- The value of the annual leave paid out to the employee will be at the final City of San Antonio rate of pay. The value of annual leave paid to University Health System would include the additional incremental cost of annual leave associated with a salary equity increase.

- Half of the costs associated with salary increases implemented by the University Health System for internal equity.
- The full cost of bringing employees to “no loss of pay” at University Health System associated with the City of San Antonio Language Skill Pay, subsequent to an internal equity increase, if necessary.
- Half of the costs associated with the funding of Post Employment Benefits
- The value of the pension contribution for University Health System for the contract term. Employee will pay their own contribution.
- The value of UHS cost of benefit program (medical, dental, vision, life insurance, disability insurance, workers compensation, unemployment compensation, employee assistance program) for the contract term. Employee will pay any associated premiums or out-of-pocket costs.
- The full one time incremental value based on the term of this contract for the employees to accrue leave at a rate determined by years of service with the City rather than accrue at the rate of a new employee at University Health System.
- Half of the cost of accrual of leave at the standard rate (8.62 per pay period), in an amount not to exceed \$229,167.00. The amount of \$36,647 will be provided at the commencement of the contract. The remaining balance will be paid at the end of the calendar year, subtracting leave used and accounting for individuals who leave UHS employment/new vacancies.
- Half the cost of physician incentives paid by UHS during the period from February 4, 2008 through December 31, 2008.

Employment Guarantee

m) University Health System will guarantee employment of transitioned City employees through December 31, 2008 except for issues of cause or loss of grant funding.

Section 7 – Funding Plan

a) For the term of February 4, 2008 to December 31, 2008, the City of San Antonio will provide funding to UHS for the management and operation of those clinics identified in Section 3 and Exhibit B of this term sheet. The City will make payment to UHS for said operations in two City Fiscal Years. Specifically, an eight (8) month funding payment will be made in FY 2008 covering February 4, 2008 through September 30, 2008. A three (3) month funding payment will be made in FY 2009 for the period of October 1, 2008 through December 31, 2008. The City will recommend for City Council approval a reduction in its Ad Valorem Tax Rate in its FY 2009 and FY 2010 Budgets commensurate with the budget amounts of the transferred functions and services. UHS will adjust its tax rate for the twelve month calendar year 2009 for the transferred functions and services. This agreement in no way waives the right of the City or UHS to increase or decrease their Ad Valorem Tax Rates as deemed necessary to keep pace with economic conditions that may affect either party's overall budget and generation of revenue.

b) The funding provided by CoSA is outlined in Exhibit E.

c) UHS will be entitled to all patient co-payments, Medicaid reimbursements and other program income earned from UHS clinic operations.

d) Beginning January 1, 2009, the Health System will be responsible for funding all of the transferred clinical preventive health services accepted from SAMHD, and as such, it is anticipated that UHS will include budget allocations for transferred clinical preventive health services beginning in its FY 2009 budget.

Section 8 – Grants/Contracts and Billing

Grants

a) SAMHD will request that all grants listed in Exhibit F be terminated effective January, 31 2008 and further request that said grants are offered to UHS beginning February 1, 2008.

b) UHS will assume sole responsibility for any grants received through this procedure. All proceeds from activities in support of these grants will be the property of UHS.

c) The Title X Male Health Grant has a component of extensive outreach and education. Incorporating a systems approach to optimal health services, SAMHD will provide the outreach and education performance measures outlined in the initial SAMHD male health grant application to UHS via Interlocal Agreement. Additionally, SAMHD and UHS will work together to assure the stated SAMHD FY08 Title X Family Planning outreach and education objectives are met. SAMHD and UHS will jointly determine a process for future coordination of Title X grant activities at least 90 days in advance of the next funding cycle.

d) UHS will provide routine prenatal care, well child services, breast and cervical cancer screening, immunizations, family planning services, and refugee health evaluations regardless of the patient's ability to pay as required by the Texas Department of State Health Services.

e) SAMHD will not apply competitively with UHS for the grants set out in Exhibit F. UHS will apply to the grantor or contracting agency when renewal opportunities and applications become available for each grant and assume full responsibility for these programs when the new terms begin. SAMHD will provide technical assistance to UHS, as needed, to support an application for grant funding, especially on grants for which UHS has not previously applied, and further will provide services and support as outlined above in paragraph (c).

f) SAMHD will not compete with UHS for the contract to provide medical screenings to enrollees of Parent, Child, Incorporated (PCI). However, UHS acknowledges that the Director of Health, as Health Authority for San Antonio and unincorporated Bexar County, will continue to provide consultation services to PCI in matters related to public health.

Billing

g) A new provider prevention division will be created by UHS within Community Medicine Associates (CMA) in order to credential SAMHD providers and to facilitate billing to Medicaid, Medicare and any other appropriate third parties for services provided in connection with transferred clinical preventive health services.

Section 9 – Ancillary Services

Courier Services

a) SAMHD and UHS will coordinate courier activities from February 4, 2008- December 31, 2008 to provide services to all sites being transitioned to UHS. A daily delivery to University Health Center Downtown will also be made to deliver lab specimens routed to that facility.

Pharmacy

b) The Health System will provide necessary pharmacy services to support the operations at the transitioning clinic sites and SAMHD will pay for said services as outlined in the Interlocal Agreement.

c) UHS will provide Class D Pharmacy consultation services to remaining SAMHD STD, TB, and Dental programs, as outlined in the Interlocal Agreement, to assure compliance with Texas Pharmacy Rules and Regulations.

d) Transferring facility locations with a current Class D Pharmacy (i.e. all facilities listed in Exhibit B with the exception of the Bob Ross Center) will transfer the management of the Class D Pharmacy to the UHS Pharmacy program.

Laboratory Services

e) Transitioning facility locations performing laboratory procedures (all those listed in Exhibit B) will transfer the management of laboratory procedures to the UHS Laboratory. These include both CLIA-waived point of service testing (performed at all service locations listed in Exhibit B) and non-CLIA waived testing (ordered at all service locations listed in Exhibit B with the exception of the Bob Ross Center).

f) UHS will continue to provide support to SAMHD laboratories for analysis of clinical specimens that are submitted for epidemiological investigation purposes.

g) SAMHD will pay for uncompensated laboratory procedures performed by UHS in transitioning clinics according to the schedule provided in the Interlocal Agreement.

Radiology

h) UHS will continue to support SAMHD radiology needs as outlined in the existing Interlocal Agreement.

Section 10 – Health Promotion/Preventive Health Programs

- a) UHS and SAMHD will work cooperatively toward integrating health promotion and disease prevention programs for the benefit of improving the overall health of the community.
- b) SAMHD as the public health authority will lead the process for setting broad community public health priorities and a plan for addressing those needs.
- c) SAMHD will establish an agenda through its population based services division that will be developed into a community strategic health plan. This will complement the SAMHD strategic plan and incorporate resources and efficiencies derived from collaboration with UHS. An initial plan outlining specific community metrics and a preliminary timeline based on an assessment by SAMHD population-based services will be presented to the JPOC for review.
- d) Sources used to guide the preventive health focus will include various elements, such as the Bexar County Community Health Collaborative (BCCHC) Community Health Assessment, the SAMHD Health Profiles, the Department of Health and Human Services' Healthy People 2010, and the JPOC Prevention Matrix of Programs.
- e) All assessment data used for evaluative purposes must be shared between both SAMHD and UHS to maximize the sources of information to establish a valid and reliable set of indicators.
- f) SAMHD will work collaboratively with UHS to ensure that population based prevention services support the clinical preventive services that will be provided by UHS and seek to provide an outcomes assessment of those services.
- g) UHS and CFHP will align its prevention programs to the broader plan led by SAMHD
- h) UHS will assume responsibility for integrating individual and group clinical prevention services into UHS's existing clinical organization. UHS's prevention programs will strategically address the UHS patient population needs.
- i) UHS will produce a report regarding the status of UHS, CFHP and SAMHD prevention programs to include UHS' five year plan for prevention. This report will include the review of existing data on community health needs and the efforts of UHS, CFHP, and SAMHD to address these needs through current programs. The final report will be issued in 2008 and will be reported to the JPOC committee for review and revisions as needed.
- j) In consultation with SAMHD, UHS may strategically relocate some of its current prevention programs into the city-owned facilities that will house UHS clinical services beginning February 4, 2008.
- k) UHS and SAMHD will jointly apply for grants related to prevention and community health programs. One organization will be designated as the grantee while the other organization will

be designated as the subcontractor to ensure the proper allocation of resources and appropriate oversight of the grant performance metrics.

Section 11 – Utilization of UHS Staff for Public Health Events/Public Health Emergencies

a) SAMHD and UHS will jointly develop a community response plan to assure that adequate staffing and resources are available from both SAMHD and UHS to meet community needs for all emergency public health hazards and community events such as:

- Natural Disasters – floods, hurricanes, heat waves, etc.
- Emergency shelter health management
- Immunization Campaigns – back to school, flu shots, and similar efforts
- Unexpected emergency situations

b) The SAMHD Director of Health or his designee shall be responsible for maintaining a copy of the written plan.

Community Health Events

c) UHS and SAMHD will develop a joint calendar of community health events that will help to prioritize allocation of staff and resources and avoid duplication. This will include such things as:

- i) Scheduled immunization campaigns (e.g., back to school, influenza immunization season); and,
- ii) Screening events to be held for purposes of identifying underlying illnesses and facilitating access to care (e.g., mobile mammography; screening for cervical cancer, diabetes, glaucoma, hypertension, and hypercholesterolemia).

Public Health Emergencies

d) Public health leadership, to include declaring a public health emergency, is the responsibility of the Director, San Antonio Metropolitan Health District (SAMHD).

e) A public health emergency is an immediate threat from a naturally occurring or intentional event that poses a high risk of fatalities or serious long-term disability to large numbers of people. This includes events with a potential major public health impact due to a substantial risk of exposure from a high level of contamination or when the mode of transmission of the infectious agent might cause public panic and social disruption.

f) The primary leadership positions at each SAMHD disaster response site, Strategic National Stockpile (SNS) Point of Dispensing Sites (PODS), and all hazard shelters will be filled by SAMHD full-time staff.

- g) University Health System (UHS) will staff appropriately trained personnel from UHS ambulatory facilities in support of an emergency response declaration by the SAMHD. SAMHD will provide the UHS Emergency Preparedness Division with a list of qualifications required and the number of personnel in each job category, and UHS will develop response teams to meet those needs. SAMHD will designate training needs for the UHS staff assigned to the response teams and assist in obtaining the needed training.
- h) UHS will identify staff designated for participation on POD/shelter teams, triage teams, or medical response teams. Identified staff will be reviewed by SAMHD to assure responders receive necessary training from SAMHD or coordinating agencies. UHS will participate in all hazards event exercises in conjunction with City and County departments to better coordinate response activities.
- i) UHS will provide a liaison to the SAMHD Incident Command Post to coordinate activities during all hazards events in cases where the Regional Medical Operations Center (RMOC) is not activated.
- j) Identified staff members will be made available by UHS for training conducted by SAMHD or coordinating agencies on the roles specified; however, the training required by SAMHD does not necessarily extend to the remainder of UHS employees. UHS will ensure that these identified staff members, and others that may be identified as necessary in the future, maintain the training necessary to serve in this capacity for any all hazard emergency response. This will include such competencies in Incident Command System (ICS), Strategic National Stockpile (SNS), all hazards event response to include hurricane response, CHEM-pack and radiological response, and others as recommended by SAMHD.
- k) Acquiring additional staff to fulfill SAMHD emergency preparedness responsibilities will be conducted through existing regional response entities and structures such as the Regional Medical Operations Center and the Bexar County Medical Society and the Medical Volunteer Coordinating Committee. These personnel include but are not exclusively represented by UHS staff.
- l) The RMOC, at the direction of SAMHD, will coordinate the distribution of state and federal pre-positioned supply and equipment caches. Any additional supplies and equipment provided by local healthcare institutions (including UHS) will be inventoried for accountability and reimbursement.
- m) UHS will be required to maintain all redundant communications systems (including satellite phones, 800 MHz radios and wireless WebEOC) to support emergency preparedness and response activities, regardless of future availability of grant funding.
- n) UHS and SAMHD will develop a joint annex to be included in each organization's emergency response plan that addresses the specific details of the job categories, training requirements, and mechanisms to ensure adequate staffing levels for any all hazard response. The annexes will also provide sufficient detail to ensure minimal delay with regard to communication and activation of an emergency response and describe the process by which that

will occur. The annex will be completed and included in each agency's response plan no later than the transition date of clinical preventive health services from SAMHD to UHS on February 4, 2008.

Emergency Preparedness Planning

o) When requested by SAMHD, UHS will facilitate consultation with infectious disease, nuclear medicine, and other expert physicians for the purposes of public health preparedness planning (e.g. pandemic influenza planning) to include laboratory consultation for certain epidemiological investigations.

p) UHS will participate in planning for mass casualty events in conjunction with SAMHD and the Bexar County Medical Examiner's Office.

Section 12 – Assuring Quality of Transitioned Services

Performance Management Plan

a) Pursuant to Texas Health and Safety Code § 121.002 et seq., SAMHD in its public health assurance role is charged to "evaluate the effectiveness, accessibility, and quality of personal and population based health services in a community." It is therefore critical that during the transition of clinical preventive services from SAMHD to UHS that evaluation and quality improvement plans be established.

b) UHS and SAMHD will jointly provide oversight of transferred services through December 31, 2008 via the JPOC. The JPOC will serve as the body to review performance monitoring data and recommend performance improvement activities as needed with input from both UHS and SAMHD representatives, as set out in Section 13.

c) A detailed performance management plan will be submitted through the JPOC to the leadership of UHS and SAMHD for a joint commitment to adhere to the plan through December 31, 2008.

d) The SAMHD Director of Health or his designee shall be responsible for maintaining a copy of the written plan.

Performance Domains, Measures, and Standards

e) Performance measures will be adopted that will assess the organizational capacity and processes associated with the provision of clinical preventive health services. The following performance domains will be assessed during the transition of clinical preventive health services from SAMHD to UHS:

- Quality of Clinical Preventive Health Services
- Accessibility of Clinical Preventive Health Services
- Equity of Clinical Preventive Health Services

- Efficiency of Clinical Preventive Health Services (to include financial efficiencies)
- Patient Satisfaction
- Clinic Staff and Provider Satisfaction

Specific measures for each of these domains have been developed with input from both UHS and SAMHD stakeholders. Measures are aligned with UHS continuous quality improvement indicators where possible to allow for comparisons across UHS clinical settings.

f) Historical SAMHD performance data, as available will be used to assess the effects of the transition of clinical preventive services, and for select indicators will serve as the minimum standard for UHS performance during the transition period.

Data Sources and Collection

g) To the extent possible, data collection utilizes existing SAMHD and UHS systems and assessment tools. However, some new data collection efforts will need to be implemented including the collection of qualitative data. The performance management plan identifies specific data collection processes, instruments, frequencies and responsible individuals associated with each measure. Primary responsibility for data collection will rest with UHS, with technical assistance and support provided by SAMHD. All data will be collected at least quarterly, with some indicators assessed on a monthly basis given the availability of data.

Data Analysis and Interpretation

h) Collected data will be provided by UHS to a subcommittee of the JPOC that will be responsible for reviewing and interpreting data, and overseeing the production of a preliminary quarterly report that will be submitted to the full JPOC. The JPOC will provide additional comments regarding the progress in transitioning services, benefits and challenges encountered, and any performance improvement activities recommended.

Reporting and Performance Improvement Activities

i) UHS and SAMHD will jointly be responsible for reporting to the City Manager, SAMHD Advisory Board of Health and UHS Board of Managers on a periodic basis the findings of the performance monitoring activities, any performance improvement activities that have been identified and will be implemented, and the status and results of any performance improvement activities previously implemented.

Section 13 – Joint Planning and Operations Council

a) The Joint Planning and Operations Council (JPOC) will be composed of at least three members of the senior management staff of SAMHD and UHS. Representatives for CMA, the UTHSCSA and other health system partners may also be appointed to this body.

b) After February 4, 2008, JPOC membership will be reassessed by both SAMHD and UHS to assure appropriate representatives are available to meet the goals of the group.

c) From February 4, 2008 through December 31, 2008 the JPOC will continue to meet at least monthly to support the following ongoing activities:

i) Provide strategic and operational oversight of the transition of clinical preventive health services from SAMHD to UHS utilizing the JPOC performance management plan. Explore opportunities to expand community input into the oversight process through a community advisory board such as the Community Translational Science Award Community Advisory Board and others that may be appropriate.

ii) Identify additional opportunities for collaboration or coordination of services to improve continuity and quality of services to Bexar County including strengthening referral systems between SAMHD and UHS for related programs, exploring models to further improve the quality of care in clinical service areas, and expanding partnerships in prevention focused programs.

iii) Continue to pursue grant and funding opportunities jointly or with well-coordinated approaches and develop a protocol to guide joint grant development and management.

iv) Provide oversight of the plans and protocols that outline the shared responsibilities of UHS and SAMHD to the community regarding emergency response to all hazards incidents as well as community health events.

v) Develop plans for increased information systems interface and data sharing to support coordination of services and community health monitoring between SAMHD and UHS and to explore opportunities to work with UTHSCSA.

vi) Develop common health system workforce competencies and evaluate opportunities for integrated workforce training.

vii) Engage additional health system and community partners in developing and documenting the vision and goals for a High Performance Health System for San Antonio which includes roles and expectations for UHS and SAMHD and the UTHSCSA, UTHSCSH-SPH.

viii) Provide a forum for discussion and facilitation for securing long-term arrangements for the acquisition or lease of facilities transitioned to UHS.

ix) Provide a forum for discussion and determination of the cost of continued provision of transitioned services by UHS beyond December 31, 2008.

Section 14 – Governing Law and Severability

a) The Terms and Obligations stated herein shall be construed under and in accordance with the laws of the State of Texas and the United States and all obligations of the parties created herein are performable in Bexar County, Texas.

b) If any clause, provision, term or obligation of this Agreement is illegal, invalid or unenforceable under present or future laws effective during the term hereof, then and in that event, it is the intention of the parties that the remainder of this Agreement shall not be affected thereby, and it is the intention of the parties to this Agreement that in lieu of each clause, provision, term or obligation of this Agreement that is illegal, invalid or unenforceable, there be added as a part hereof a clause, provision, term or obligation as similar in terms to such illegal, invalid or unenforceable clause, provision, term or obligation as may be possible and be legal, valid and enforceable.

Exhibit A: Medical Staff and Prevention Program Organization

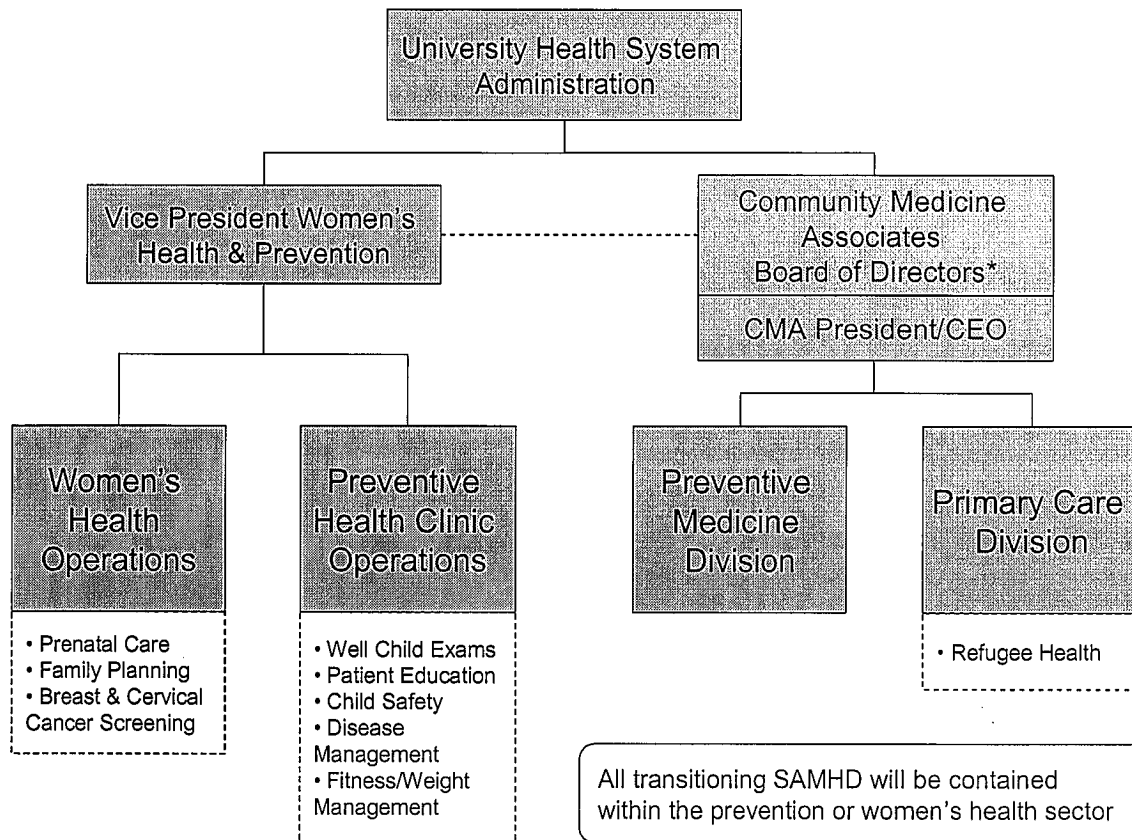


Exhibit B: Clinical Preventive Health Service Sites

City Facilities				
Clinic	Location	Services Provided	Space Allocated	Shared Space
Bob Ross Center	2219 Babcock 78229	Adult Health	2,415	460
Eastside Branch Clinic	210 N. Rio Grande 78202	Refugee Screening	3,699	3,222
Kenwood Clinic	302 Dora St. 78212	Adult Health, Dental, Family Planning, Maternity, Well Child, Immunizations,	3,795	1,176
Naco-Perrin Clinic	4020 Naco-Perrin Boulevard	Adult Health, Family Planning, Maternity, Well Child, Immunizations,	7,355	395
Old Highway 90 Clinic	911 Old Highway 90 West 78237	Adult Health, Family Planning, Maternity, Well Child, Immunizations,	5,554	0
Pecan Valley Clinic	802 Pecan Valley Dr. 78220	Adult Health, Family Planning, Maternity, Well Child, Immunizations, WIC	3,113	2,079
South Flores Clinic	7902 S. Flores St. 78221	Adult Health, Family Planning, Maternity, Well Child, Immunizations	5,940	0
Southwest Branch Clinic*	9011 Poteet-Jourdanton Freeway	Dental, WIC	9,522	1,900
Frank Garrett Center	1226 NW 18th St. 78207	Adult Health, Dental, Family Planning, Maternity, Well Child, Immunizations,	1,899	1,241
Zarzamora Clinic	4503 S. Zarzamora 78211	Adult Health, Family Planning, Maternity, Well Child, Immunizations, WIC	4,959	2,335
Non - City Facilities				
Salinas Clinic	630 S. Gen. McMullen 78237	Adult, Dental, Maternity, Immunizations, Well Child, WIC	3,053	3,773

* clinic area currently being leased by CentroMed

ADMINISTRATIVE DIRECTIVE NO. 7.3

EFFECTIVE DATE: January 1, 1990

REVISION DATE: OCTOBER 05, 1988

SUBJECT: DATA SECURITY POLICIES AND PROCEDURES

1. PURPOSE:

This directive establishes policy and fixes responsibility for ensuring the security, privacy, and confidentiality of data maintained by City departments in computerized systems.

2. RESPONSIBILITIES:

A. The Information Resources Department shall be responsible for developing, maintaining, publishing and administering a comprehensive DATA SECURITY PLAN. This plan shall reference applicable statutes, ordinances and Administrative Directives pertaining to Data Security. At least industry standards for security, integrity and recovery shall be adopted and strictly enforced. The plan shall be applicable to remote sites or facilities in all City offices or spaces and shall ensure that unauthorized access to City data processing resources is prohibited. The plan shall include audits and intrusion detection procedures.

B. The Information Resources Department, through its Data Administration function, shall serve as the contact point and coordinator for data sharing among City departments and dissemination of data on magnetic media to the public and other agencies.

D. The Owner of the Data shall be responsible for:

Determining the sensitivity classification for all data.

Establishing procedures for dissemination of data to the public from computerized systems for the Owner's department in compliance with Administrative Directive 1.31, Open Records.

Approving or developing procedures for backup and recovery.

Approving on-line access by other users.

EFFECTIVE DATE: January 1, 1990

REVISION DATE: OCTOBER 05, 1988

SUBJECT: DATA SECURITY POLICIES AND PROCEDURES PAGE 2

2. RESPONSIBILITIES: Cont'd)

Developing an availability impact statement for all computerized systems. This statement will briefly outline the impact on the department's operation if the computer system supporting a function is inoperative.

Establishing and enforcing procedures designed to insure the integrity of the data contained in computerized files.

Approval and responsibility for all software developed or procured from any source other than the Information Resources Department.

D. The User is responsible for:

Safeguarding the City's data resource.

Complying with the provisions of the SECURITY PLAN and relevant Administrative Directives.

3. POLICY:

A. The data and information in the City's computerized systems, along with the hardware and software required to process the data, are a valuable resource and represent a significant investment.

B. All reasonable precautions shall be taken to insure the security of the data and of the software; and to protect the privacy and confidentiality of the data while allowing reasonable access and dissemination policies which are consistent with applicable statutes, ordinances and directives.

4. APPLICABILITY:

For the purpose of this Directive, the following are deemed to be the property of the City of San Antonio and are subject to the provisions of this Directive:

EFFECTIVE DATE: January 1, 1990

REVISION DATE: OCTOBER 05, 1988

SUBJECT: DATA SECURITY POLICIES AND PROCEDURES PAGE 3

4. APPLICABILITY: (Cont'd)

- A. All computer hardware, Data Communications devices of whatever nature, procured with City funds, residing on City property or used in the conduct of City business.
- B. All software, firmware or other data processing entity, system description, program description, software documentation or other documents developed by City personnel or with City funds or licensed to the City of San Antonio.
- C. All data from whatever source and in whatever form which is entered into, stored by, processed by or retrieved from or through any City computer.

5. DATA CLASSIFICATION:

All data shall be classified as Public, Operational, or Confidential for the purpose of establishing dissemination guidelines. Administrative Directive 1.31 places responsibility for developing and updating the Municipal Open Records Policy and Fire and Police Open Records Policy with the City Attorney. This responsibility includes responding to requests for opinions on whether or not records are public under the Open Records Act. Classification of data shall conform to those guidelines.

A. CONFIDENTIAL DATA

Data in this classification is that which may not be disseminated or which has restricted dissemination, mandated by Statute, Ordinance, Court Order or Directive.

B. OPERATIONAL

Data which is specifically exempted from the Texas Open Record Law.

C. PUBLIC

All data and information not classified as CONFIDENTIAL or OPERATIONAL.

ADMINISTRATIVE DIRECTIVE NO. 7.3

EFFECTIVE DATE: January 1, 1990

REVISION DATE: OCTOBER 05, 1988

SUBJECT: DATA SECURITY POLICIES AND PROCEDURES

PAGE 4

6. DISSEMINATION GUIDELINES:

A. PUBLIC DATA

This data may be disseminated to anyone requesting the data as follows:

The Owner, or designated employee, of the data may disseminate the data or information derived from the data to anyone. Fees may have been established by ordinance for this service.

All City departments may have access to this data. However, the requesting department shall submit a request in writing to the Data Administrator who will notify the Owner and insure the operational integrity of the data.

All requests for data to be provided on magnetic media shall be made to the Data Administrator. The Owner of the data will be notified in writing of the request and be informed of the data provided and to whom it was provided.

All requests for copies of software, program descriptions, system descriptions or other computer related documentation shall be made to the Data Administrator who will maintain a list of such disseminations.

B. OPERATIONAL DATA

Data in this classification usually consists of incomplete work products of the City and other data which is exempt from the Open Records Law. The following rules apply:

No employee shall disseminate data in this classification without authorization from the Department Head or City Attorney.

This data may be shared with other City departments. However, the requesting department must submit a request to the Data Administrator. If the Owner agrees to share the data, the Data Administrator will insure that adequate protection for the data is in place.

ADMINISTRATIVE DIRECTIVE NO. 7.3

EFFECTIVE DATE: January 1, 1990

REVISION DATE: OCTOBER 05, 1988

SUBJECT: DATA SECURITY POLICIES AND PROCEDURES PAGE 5

6. DISSEMINATION GUIDELINES: (Cont'd)

B. OPERATIONAL DATA (Cont'd)

Systems shall be designed in such a way as to insure the privacy of data within this classification.

C. CONFIDENTIAL DATA

Data within this classification usually consists of data which is prohibited from disclosure by statute, court order or decision, ordinance, or Administrative Directive, and is generally that which would violate the rights of citizens or compromise the City in fulfilling its obligations.

This data may not be disseminated by any employee.

This data may not be shared with other departments, except by written authorization by the City Manager.

The Data Administrator shall insure that extraordinary procedures are employed to protect the confidentiality of this data.

7. PROHIBITIONS:

- A. No employee shall use anything subject to this Directive for personal gain.
- B. No employee shall intentionally or knowingly access or attempt to access any City data without having both the right and the need to access such data.
- C. No employee shall add, update or delete or attempt to add, update or delete any record or data within any data file, data base or system without having a legitimate City business need and proper authorization to do so.

ADMINISTRATIVE DIRECTIVE NO. 7.3

EFFECTIVE DATE: January 1, 1990

REVISION DATE: OCTOBER 05, 1988

SUBJECT: DATA SECURITY POLICIES AND PROCEDURES PAGE 6

7. PROHIBITIONS: (Cont'd)

- D. No employee shall disseminate any data subject to this Directive unless such dissemination complies with the guidelines in paragraph 6.0.
- E. No employee shall make any copy of any software, system documentation, program description or any other descriptive material for dissemination unless such dissemination complies with the guidelines in paragraph 6.0.
- F. No employee shall procure, obtain or use in any manner any software developed by non-City personnel, or any City computer without having the proper licenses and approval from the Owner of the Data and the Department Head having custody of the computer.
- G. No employee shall discuss the details of the SECURITY PLAN or disclose any program name, access code, user identification, password, telephone number or any other item of information that may compromise the City's Data Processing Resources or Data.
- H. No employee shall knowingly permit any other person to violate any provision of this Directive.

8. PENALTIES:

Violation of any of the Prohibitions outlined in Section 7 above, shall result in disciplinary action. Administrative action may range from a reprimand and loss of access privileges to termination of employment. Violations may also result in civil and/or criminal prosecution.

9. DEFINITIONS:

- A. DISSEMINATE - to communicate, by any means, information of any kind to any person or entity who is not authorized to directly access the information at its source;

EFFECTIVE DATE: January 1, 1990

REVISION DATE: OCTOBER 05, 1988

SUBJECT: DATA SECURITY POLICIES AND PROCEDURES PAGE 7

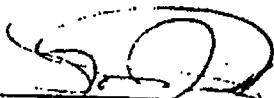
9. DEFINITIONS: (Cont'd)

- B. OWNER - The department or other organization responsible for creating and maintaining a specific item of data.
- C. USER - Anyone who has access to an item of data from any City file or has access to any other City Data Processing resource.

APPROVED:



FRANK A. STROMBOE, Director
Information Resources Department



LOUIS J. FOX, City Manager
City Manager's Office

ADMINISTRATIVE DIRECTIVE 7.4

Acceptable Use of Electronic Communications

Effective Date: November 30, 2005

Revision Date(s):

I. PURPOSE:

This Administrative Directive provides guidance for the use of electronic communications systems, including electronic mail and internet access, operated and maintained by the City of San Antonio. This Directive supports and supplements Administrative Directive 7.5 – Acceptable Use of Information Technology. Nothing in this Directive supersedes provisions of Directive 7.5.

II. POLICY:

- A. The City of San Antonio provides e-mail services and internet access to its employees as tools to perform business-related activities. All users of the City's electronic communications systems, including its internet access facilities, are responsible for using that technology in an appropriate and lawful manner. **Any activity performed on a workstation under an employee's login ID is presumed to be performed by that employee and is the responsibility of the employee.**
- B. The City will manage its electronic mail records in accordance with Texas Administrative Code, Chapter 7, Sections 7.71-7.79 and Local Government Code, Chapter 205, Sections 205.001-205.009 (Local Government Bulletin, B, Electronic Records Standards and Procedures.).
 - Most e-mail messages are not essential to the fulfillment of statutory obligations or to the documentation of the city's functions and may be deleted. These messages may include personal messages, internal meeting notices, letters of transmittal, and general FYI announcements.
 - Messages which do fulfill statutory obligations or document the City's functions are subject to retention and disposition requirements established by the Texas Administrative Code.
- C. The City's internet connection is a shared resource that serves all its employees and provides the general public with access to its web site. Inappropriate use of internet resources reduces the usefulness of this resource to its employees and citizens.
- D. City electronic mail and internet systems are for official business use. Users may make and receive personal communications during business hours that are necessary and in the interest of the City. While some incidental use (as defined in AD 7.5) of City-managed technology is unavoidable, such incidental use is not a right, and should never interfere with the performance of duties or service to the public.

III. DEFINITIONS

- A. **Electronic mail record:** An electronic government record sent and received in the form of a message on an electronic mail system of a government, including any attachments, transmitted with the message.
- B. **Local Government Record Retention Schedules:** Publications issued by the Texas State Library and Archives Commission under the authority of Subchapter J, Chapter 441 of the Government Code which establish the mandatory minimum retention period for a local government record.

ADMINISTRATIVE DIRECTIVE 7.4**Acceptable Use of Electronic Communications**

Effective Date: November 30, 2005

Revision Date(s):

- C. Records Management Officer: The person who administers the records management program established in each local government under Local Government Code, Chapter 203, Section 203.026.
- D. Retention period: The minimum time that must pass after the creation, recording or receipt of a record or the fulfillment of certain actions associated with a record, before it is eligible for destruction.

IV. POLICY GUIDELINES:

This directive applies to all users of the City's electronic mail and internet access systems who connect to the City's network in order to use those facilities. All electronic messaging equipment or technology that is owned or administered by the City is included within this Directive's scope.

V. RESPONSIBILITIES:**Information Technology Services Department**

- A. Organizational responsibility for the development, implementation, maintenance, and compliance monitoring of this directive is placed with ITSD and the City Clerk's Office.
- B. ITSD and Human Resources will provide City departments with initial communication and training regarding application of this directive. However, City Department Directors are ultimately responsible for communicating the policies and standards established in this AD to all personnel in their respective departments and for ensuring compliance within their respective departments with those policies and standards.
- C. ITSD is responsible for communicating the policies and standards established in this directive to all third-party users (contractors, consultants, agencies having a contractual relationship with the City) and for ensuring their compliance. Those City departments who work with the third-party users are responsible for identifying the third-party users to ITSD.
- D. ITSD will archive undeleted messages after 90 days.
- E. ITSD may terminate e-mail services to any user if he/she is found in breach of this directive. Service may be restored to the employee following a written request by the employee's Department Director.

Office of the City Clerk

In cooperation with the ITSD, the Records Management Officer will ensure that appropriate training and communication of the requirements for retention, maintenance, and disposition of records is made available for staff.

Department Directors and Their Designees

- A. Departments are responsible for implementation, training, and enforcement of the data classification standards defined by the Texas State Attorney General's Office as

ADMINISTRATIVE DIRECTIVE 7.4**Acceptable Use of Electronic Communications**

Effective Date: November 30, 2005

Revision Date(s):

they apply to information stored on City-administered technology or equipment including data retention and disposition.

- B. Department Directors are responsible for any disciplinary actions taken against employees who violate this policy. The Human Resources Department will provide guidance as required to City departments regarding appropriate disciplinary actions to be taken against employees who violate this policy

Employees

- A. Employees shall, with guidance and training from the Records Management Officer, manage e-mail messages according to the City's approved retention periods.
- B. Employees who voluntarily terminate employment, retire, or are transferred, will be required to review their e-mail accounts with their supervisor. The employee's supervisor is responsible for ensuring that e-mail records are properly classified and stored, and that working or convenience copies are disposed of in the prescribed manner.

Human Resources

- A. Human Resources will provide guidance to departments for disciplinary actions associated with violations of the directive.
- B. Human Resources will assist ITSD in providing training regarding this directive to current and future employees. Following implementation of this directive, Human resources will ensure that all new employees are provided a copy of this directive.
- C. The Human Resources Director will consult with the Chief Information Officer in approving any monitoring of systems for personnel reasons.

VI. PROCEDURES:

- A. All electronic mail messages sent, received or stored on the City's systems are considered City property and may be read at any time. Messages may be furnished to third parties in order to comply with requirements of the Texas Public Information Act. All internet activity is logged, and logs may be inspected at any time.
- B. Security and proprietary information
 - 1. The use of HTML formatting for e-mail messages is prohibited.
 - 2. E-mail attachments that may constitute a risk to the City's technology environment will be removed from e-mail messages passing through the City's mail servers. Removed attachments are replaced by a message indicating that they have been removed and the header and text of the original message delivered normally.
 - 3. A spam message filter is used to reduce the transmission of chain letters, broadcast announcements, general advertisement postings, or any other message via e-mail to a group of persons not requesting the message.
- C. Unacceptable Use

ADMINISTRATIVE DIRECTIVE 7.4**Acceptable Use of Electronic Communications**

Effective Date: November 30, 2005

Revision Date(s):

The following activities are prohibited unless performed in the course of legitimate job responsibilities. The list below is by no means exhaustive, but provides a framework for activities which fall into the category of unacceptable use-

1. Engaging in any activity that is illegal under local, State, or Federal statutes or which violates City of San Antonio policies and Administrative Directives.
2. Using, accessing, or transmitting pornographic or sexually-explicit materials, offensive threatening, racial or hate language or images.
3. Engaging in any form of harassment, whether sexual or otherwise, or sending any unwelcome personal communication. It is the perception of the recipient that prevails, not the intent of the sender.
4. Any personal use that interrupts City business and that keeps an employee from performing his/her work. **Employees should not use their City electronic mail account as their primary personal e-mail address.**
5. Extensive personal use of the internet for any non work-related purpose during working hours which decreases the employees productivity or results in decreased performance of the City's internet facilities.
6. Unauthorized downloading of and distributing of copyrighted materials.
7. Downloading or copying music, photographs or video material, including such material that has been obtained legally, onto City computers or servers.
8. Downloading and/or installing executable program files from the internet without the approval of ITSD.
9. Unauthorized reading, deleting, copying, modifying or printing electronic communications of another user.
10. Using the City's electronic mail or internet systems for private gain or profit.
11. Using personal software which allows peer-to-peer communications between two workstations (eg., online chat, KaZAA, etc.).
12. Using instant messaging through public service providers.
13. Using City systems for personal access to auctions (such as e-Bay).
14. Soliciting for political, religious, or other non-business uses not authorized by the City.
15. Accessing non-business related streaming media, including internet-based radio.
16. Accessing any non-business related application which maintains a persistent connection to the internet, such as "Weather Bug", stock tickers, etc.
17. Using City electronic mail or internet facilities for political purposes, including voting. (This does not include the use of equipment for public voting at City facilities).
18. Including email "tag lines" or personal quotations other than ones that state the mission of the City or the user's Department.

19. Sending or forwarding junk e-mail, chain letters, or other mass mailings.
20. Sending or receiving e-mail through non-City managed e-mail systems (e.g. Hotmail or Yahoo) while at work.

VII. RETENTION AND DISPOSITION OF E-MAIL

The City's approved Declaration of Compliance with the Local Government Records Retention Schedules establishes record series and the retention period for each series. It is the content and function of an e-mail message that determines the retention period for that message. All e-mail sent or received by a government is considered a government record. Therefore, all e-mail messages must be retained or disposed of according to the City's retention requirements. E-mail systems must meet the retention requirement found in Texas Administrative Code, Chapter 7, Section 7.77.

Employees and their supervisors should seek guidance from the City's Records management Officer if there is a question concerning whether an electronic message should be deleted.

VIII. PRIVACY AND MONITORING

- A. The City does not routinely monitor the content of electronic communications systems, but may do so without notice. City systems may be monitored to support operational, maintenance, auditing, security and investigative activities, including enforcement of this Directive, legal requests, public records requests, or other business purpose. ITSD staff may monitor network infrastructure, servers and workstations for the purpose of maintaining system reliability, availability and security.
- B. Only Department Directors or higher may request access and monitoring of City administered technology or communications systems for employees under their supervision. Unauthorized monitoring or reading of electronic communications systems or their contents violates this Directive.
- C. Any request to monitor must be approved by the Chief Information Officer (CIO) and the Human Resources Director prior to the commencement of monitoring.
- D. To obtain the necessary authorization, a written request from the requestor to the Human Resources Director must include:
 1. The stated purpose for accessing and/or monitoring.
 2. A specific description of the systems or content to be accessed or monitored (e.g. the name of the mailbox earmarked for review – exactly as it appears in the e-mail directory).
 3. Name and phone number of the employee in the requesting department who is responsible for coordination of the request.
- E. The Human Resources Director will forward the request to the CIO for concurrence.

- F. The CIO will assign staff from ITSD to assist as necessary with any authorized access and monitoring activities.

IX. INTERNET FILTERING AND WAIVER REQUESTS

The City uses filtering software to block access to certain internet sites that have been determined by the Management Team to be inconsistent with most employee job responsibilities and other City policies. There may be specific circumstances in which blocking is too restrictive to allow an employee or group of employees to adequately perform their duties. In these cases, a waiver from the policy must be requested. To request a waiver:

- A. Employee should complete the on-line site access request form that is available when attempting to access a blocked site.
- B. The Chief Information Officer or his designee will review the request in a timely manner, and will verify the business need with the employee's Department Director or Management Team member as may be appropriate. The Chief Information Officer may request guidance from Human Resources and/or Legal Departments as may be necessary.
- C. The approved request will be maintained by ITSD.
- D. If the requested access will allow an employee to perform activities which are normally prohibited by City policies, the employee's Department Director must submit a request for waiver in writing to the Chief Information Officer. The waiver request must include a statement that the Department Director is aware of any increased risks that will result from the waiver, and has added appropriate controls to adequately reduce the additional risks.

X. DISCIPLINE:

- A. Failure to comply with this directive will result in disciplinary action in accordance with the Municipal Civil Service Rules of the City of San Antonio, Rule XVII, Section 2. Discipline will be evaluated and based upon the number of violations and severity of the incident. The Human Resources Department must be consulted by a department when assessing the appropriate level of disciplinary action.
- B. Employees who fail to follow and administer this directive will be disciplined under the authority of the Department Director.
- C. This Administrative Directive does not supersede the Department Director's authority over the determination of final disciplinary actions taken, particularly in cases where the safety of the general public or City employees are significantly compromised by an infraction of this Administrative Directive. A Department Director may choose to assess more severe disciplinary action against an employee depending on the severity of the infraction.

ADMINISTRATIVE DIRECTIVE 7.4

Acceptable Use of Electronic Communications

Effective Date: November 30, 2005

Revision Date(s):

This directive supersedes all previous correspondence on this subject. Information and/or clarification may be obtained by contacting the ITSD Department at 207-8301.




Hugh Miller, Jr., Interim Director ITSD

11/29/05

Date

Approved by:



Michael Armstrong, Chief Information Officer

11/29/05

Date

Approved by:



Sheryl Sculley, City Manager

11-29-05

Date

ADMINISTRATIVE DIRECTIVE 7.5 Acceptable Use of Information Technology

Effective Date: December 1, 2005

Revision Date(s):

I. PURPOSE:

The purpose of this Administrative Directive (AD) is to provide guidance regarding the acceptable use of computer equipment, networks and other information technology hardware and software in the City of San Antonio ("City").

II. POLICY

- A. The City provides access to its technology systems to assist technology users in performing their duties efficiently and effectively. Inappropriate use of information technology exposes the City to internal and external risks and may reduce the effectiveness of those systems. All users of City-owned and managed information technology are responsible for using that technology in an appropriate and lawful manner. Any activity performed on a workstation under an employee's login ID is presumed to be performed by that employee.
- B. There should be no expectation of privacy in the use of City-administered technology or equipment. Due to the City's need to protect resources and assets, and its obligation to comply with Texas Public Information Act (Chapter 552, Texas Government Code) open records requirements, there is no expectation of confidentiality of information maintained on any storage or network device belonging to the City unless it is specifically protected by law from disclosure and then only to the extent of that legal protection.
- C. All information generated by or stored on city-provided equipment is the property of the City of San Antonio. There should be no expectation of confidentiality with regard to any files, including email, stored on any City-managed computer.
- D. Technology users shall use City-managed technology for official business, but may make and receive personal communications, including telephone calls during business hours, that are necessary and in the interest of the City. While some incidental use (as defined below) of City-managed technology is unavoidable, such incidental use is not a right, and should never interfere with the performance of duties or service to the public.
- E. This Directive will support existing and forthcoming technology-related Directives, and will apply to all users of the City's information technology and networks unless otherwise specified in this document.

III. DEFINITIONS:

- A. City: The City of San Antonio, its departments and agencies.
- B. City-administered technology or equipment: Any technology or equipment that is used and/or managed by the City even if the City does not own said technology or equipment. City-managed technology includes technology or equipment owned by the City, on loan to the City, funded by grants, leased by the City, etc. Technology includes, but is not limited to, computers, mobile communication devices, telecommunication devices, servers, networks, software, databases and e-mail messages.

ADMINISTRATIVE DIRECTIVE 7.5 Acceptable Use of Information Technology

Effective Date: December 1, 2005

Revision Date(s):

- C. DSS: The person who is filling the role of technical specialist for a department. This role is typically called a Department Systems Specialist (DSS) or Department Systems Manager (DSM).
- D. E-mail spoofing: Forging an e-mail header to make it appear as if it came from someone other than the actual source.
- E. Federal statutes: The laws of the United States and/or the country where the user is located.
- F. Incidental personal use: Any personal use of City-owned or managed technology that:
 - a) does not cause any additional expense to the City;
 - b) is infrequent and brief;
 - c) does not have a negative impact on overall employee productivity;
 - d) does not interfere with the normal operations of an employee's department or work unit;
 - e) does not compromise the City in any way;
 - f) does not embarrass either the City or the employee;
 - g) does not contravene other elements of this policy; and
 - h) serves the interests of the City in allowing employees to address important personal matters which cannot be addressed outside of work hours without leaving the workplace.

Examples of personal communications that could be in the interest of the City include:

- a) communications to alert household members about working late or other schedule changes;
- b) communications to make alternative child care arrangements; communications with doctors, hospital staff, or day care providers;
- c) communications to determine the safety of family or household members, particularly in an emergency;
- d) communications to make funeral arrangements;
- e) communications to reach businesses or government agencies that can only be contacted during work hours;
- f) communications to arrange emergency repairs to vehicles or residences.

City departments, in consultation with the Human Resources Department, may determine whether a use is personal or business and if usage is personal, whether it is incidental.

- G. ITSD: the City's Information Technology Services Department or successor agencies.

ADMINISTRATIVE DIRECTIVE 7.5 Acceptable Use of Information Technology

Effective Date: December 1, 2005

Revision Date(s):

- H. Local statutes: The ordinances, statutes, and laws of the City, Bexar County and/or the municipality or county where the user is located.
- I. Malware: Short for **malicious software**, software designed specifically to damage or disrupt a system, such as a virus, worm, Trojan horse, or e-mail bomb.
- J. Network: A group of two or more computer systems linked together to facilitate communication, data sharing and processing among the systems.
- K. Phishing: The act of sending an e-mail falsely claiming to be an established legitimate enterprise in an attempt to manipulate someone into surrendering private information that can be used for identity theft or other malicious purposes. The e-mail directs the receiver to a web site that appears to be owned by the legitimate enterprise and asks for private information to be used in identity theft or other malicious purpose.
- L. Public access terminals: Computers provided by City for use by the general public.
- M. Spam (called "unsolicited commercial electron mail messages" as it is defined by the State of Texas statutes): A commercial electronic mail message sent without the consent of the recipient by a person with whom the recipient does not have an established business relationship. The term does not include electronic mail sent by an organization using electronic mail for the purpose of communicating exclusively with members, employees, or contractors of the organization.
- N. State statutes: The statutes and laws of the state of Texas and/or the state where the user is located. Where statutes from two states conflict, the statutes of the State of Texas shall take precedence.
- O. Technology user: Any employee, contractor, consultant, part-time or temporary employee who uses City-administered technology or equipment, and anyone accessing the City's networks, exclusive of the City's web pages.

IV. POLICY GUIDELINES:

This Directive applies to any party using city-owned or city-managed technology, or any party connecting to the City's networks. All equipment or technology that is owned or administered by the City is included within this AD's scope. Public access terminals provided by the City are **not** included in the scope of this policy, except where those terminals are used by City staff to access the City's networks.

RESPONSIBILITIES:

Information & Technology Services Department

- A. Organizational responsibility for the development, implementation, maintenance, and compliance monitoring of requirements established in this Directive is placed with the Information & Technology Services Department (ITSD).
- B. ITSD, along with the Human Resources Department, will provide City departments with initial communication and training regarding this Directive. However, Department Directors are ultimately responsible for communicating the policies and standards established in this Directive to all personnel in their respective departments

ADMINISTRATIVE DIRECTIVE 7.5 Acceptable Use of Information Technology

Effective Date: December 1, 2005

Revision Date(s):

and for ensuring compliance within their respective departments with those policies and standards.

- C. ITSD may disconnect any computer from the City network at any time if continued connectivity constitutes a threat to the City or City-administered technology or equipment. ITSD will attempt to contact the DSS responsible for the computer prior to disconnecting as long as such notification does not allow further degradation of the City-administered technology or equipment. Such notification will be made after the disconnection if prior coordination was not possible.

Department Directors and their designees

- A. Department Directors are responsible for any disciplinary action taken against employees who violate this Directive in accordance with section VI. The Human Resources Department will provide guidance as required to City departments regarding appropriate disciplinary action to be taken against employees who violate this policy.

Office of the City Clerk

- A. The Office of the City Clerk is responsible for the creation, maintenance and administration of all rules regarding the classification and protection of information stored on City-administered technology or equipment.

Employees

- A. Employees are accountable for the proper use of City-owned technology, and should be aware that they are responsible for any information that they generate or distribute through the City's technology systems. Any activity performed on a workstation under an employee's login ID is presumed to be performed by that employee.
- B. Employees should be aware that all information generated by or stored on city-provided equipment is the property of the City of San Antonio. There should be no expectation of confidentiality with regard to any files, including email, stored on City computers. Any materials stored on City equipment may be monitored and reviewed by City management at any time.
- C. Employees should be aware that most information generated and stored on City-provided equipment is subject to applicable open records laws.

Human Resources

- A. Human Resources will provide guidance to departments for disciplinary actions associated with violations of the Directive.
- B. Human Resources will assist ITSD in providing training regarding this directive to current and future employees. Following implementation of this directive, Human

ADMINISTRATIVE DIRECTIVE 7.5 Acceptable Use of Information Technology

Effective Date: December 1, 2005

Revision Date(s):

resources will ensure that all new employees are provided a copy of this directive and complete the attached acknowledgement.

- C. The Human Resources Director will consult with the Chief Information Officer in approving any monitoring of systems for personnel reasons.

V. PROCEDURES:

A. General use and ownership of information technology

1. City-administered technology and equipment is for use in conducting City business with the exceptions noted in this Directive. Technology users should be aware that the data they create, receive, or forward on the City's systems remains the property of the City.
2. Incidental personal use (as defined in this Directive) of City-administered technology or equipment is permissible as long as it does not interfere with the performance of assigned duties, does not have a detrimental effect on City information technology and systems, and is not prohibited by this policy. Personal use should be limited to those necessary activities described in the definition of "Incidental Use" above.
3. Supervisors are responsible for monitoring the incidental personal use of information technology by their employees. If departmental management determines an employee's usage is not allowable as incidental personal use, management should notify the employee immediately. Continued unacceptable personal use by that employee shall be disciplined in accordance with section VI. If an employee is not sure usage is acceptable, he/she should consult his/her supervisor for guidance.
4. There should be no expectation of privacy in the use of City-administered technology or equipment. Because of the City's need to protect its resources and assets and its obligation to comply with Texas Public Information Act (Chapter 552, Texas Government Code) open records requirements, there should be no expectation of confidentiality of information maintained on any storage or network device belonging to the City unless it is specifically protected by law from disclosure and only then to the extent of that legal protection.
5. The City does not routinely monitor employee use of City-owned and managed technology. However, the Chief Information Officer or his/her designee may monitor City-administered technology or equipment at any time for security, network maintenance or audit purposes, with or without consent of the technology user. Monitoring of technology usage for personnel-related matters shall require the approval of the Chief Information Officer and the Human Resources Director.

B. Security and proprietary information

1. Information stored on City-administered technology or equipment should be classified in accordance with federal, state, and local statutes, ordinances, and policies regarding the confidentiality of the information as prescribed by the Office of the City Clerk. Employees should take the necessary steps or follow prescribed processes to prevent unauthorized access to confidential information. Unclassified information should not

ADMINISTRATIVE DIRECTIVE 7.5 Acceptable Use of Information Technology

Effective Date: December 1, 2005

Revision Date(s):

be released to non-City entities without authorization and approval by the City Manager's Office.

2. Employees must comply with all City Directives regarding use of information technology, including forthcoming Directives related to:
 - a. Electronic Communications (e-mail, voice and internet)
 - b. Password Management
 - c. Security
 - d. Data management and Classification
 - e. Monitoring
 - f. Remote Access
3. All personal computers, laptops and workstations should be protected from unauthorized access when the system is unattended. The recommended method of securing the device is with a password-protected screensaver (with the automatic activation feature set to 15 minutes or less) or by manually locking the device (Ctrl-Alt-Delete for Windows 2000 or XP users). Devices that cannot be locked as described above should be secured by logging off the devices or turning them off.
4. Employees must take reasonable and necessary precautions to secure and protect portable devices. Protect portable devices in accordance with the following guidelines:
 - a. Laptops and other portable devices used in an office setting should be locked in a drawer or cabinet or should be secured to the desktop with a device manufactured for that purpose.
 - b. Users should retain physical contact with all portable devices in areas where the risk of theft is high such as airports and hotels.
 - c. If a portable device must be left unattended in a vehicle, it should be locked in the vehicles trunk or otherwise secured and protected from plain view inside the locked vehicle.
 - d. Portable devices should never be left in a vehicle, even if locked and out of sight, overnight. Reasonable precautions should be taken to protect the device when traveling, even if the travel is local.
5. ITSD regularly maintains operating systems, updates anti-virus software, and applies security patches by sending those updates during the evening hours to computers attached to the network. When an employee leaves for the day, he/she should log off from his/her computer, but should leave the computer turned on and attached to the network. Because laptops may be secured during non-business hours and may not be connected to the network when updates are sent, users should work with their DSS to ensure updates to portable devices are installed in a timely manner.
6. All technology devices used by a technology user to connect to the City's networks shall continually execute approved virus-scanning software with a current virus definition file. This includes employee-owned equipment attached to the City's

ADMINISTRATIVE DIRECTIVE 7.5 Acceptable Use of Information Technology

Effective Date: December 1, 2005

Revision Date(s):

networks through remote access technologies. The City is not responsible for providing the required virus-scanning software for employee-owned computers.

C. Unacceptable use

The following activities are prohibited unless performed in the course of legitimate job responsibilities. The list below is by no means exhaustive, but provides a framework for activities which fall into the category of unacceptable use:

1. Engaging in any activity that is illegal under local, state, or federal statutes or which violates City of San Antonio policies and Administrative Directives;
2. Accessing, displaying, storing or transmitting material that is offensive in nature, including sexually explicit materials, or any text or image that can be considered threatening, racially offensive, or hate speech. This includes any images, text, files, etc. sent via email to co-workers or outside parties. **Accessing, storing, displaying, or transmitting pornographic materials using City-owned and managed technology is strictly forbidden;**
3. Any personal uses that interrupt City business, or which prevents an employee from performing his/her work. Employees should not use City e-mail accounts as their primary personal e-mail address. City systems shall not be used to chat online, "blog", or shop online;
4. Violating any copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by the City;
5. Unauthorized reading, deleting, copying or forwarding of electronic communications of another, or accessing electronic files of another without authorization;
6. Sending SPAM to either internal or external parties;
7. Unauthorized duplication of copyrighted material including, but not limited to, text and photographs from magazines, books or other copyrighted sources, copyrighted music and/or copyrighted movies. Copying or installing copyrighted software for which the City or the end user does not have an active license is not permitted;
8. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws;
9. Maliciously introducing malware or similar programs into the network or server;
10. Revealing a City account password to others or allowing use of a City account by others. This includes household members and visitors when work is being done at home. Revealing a City account password to an authorized technician during troubleshooting procedures is not a violation of this policy. In such a situation, a new password should be established as soon as possible after the problem is resolved;

ADMINISTRATIVE DIRECTIVE 7.5 Acceptable Use of Information Technology

Effective Date: December 1, 2005

Revision Date(s):

11. Making fraudulent offers of products, items, or services originating from any City account
12. Using City-owned technology for political activity, private gain, gambling, shopping, games or other entertainment, or any other non-business function unless permitted by this Directive;
13. Causing security breaches or disruptions of City communications. Security breaches include, but are not limited to:
 - a. Accessing data which the employee is not authorized to access or logging into a server or user account that the employee is not expressly authorized to access;
 - b. Causing network disruptions for malicious purposes including, but not limited to, network sniffing, ping floods, packet spoofing, denial of service, and forged routing information for malicious purposes;
 - c. Port scanning or security scanning for malicious purposes is prohibited. Non-malicious scanning that is part of a City-sanctioned security process is allowed. ITSD should be notified prior to any such scanning;
 - d. Circumventing user authentication or security of any device, network or account;
 - e. Maliciously interfering with or denying service through denial of service attack, or other means;
 - f. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, another user's device or session, via any means, locally or via the City's network;
 - g. Adding/removing hardware components, attaching external devices, or making configuration changes to information technology devices without approval by ITSD.

VI. DISCIPLINE (if applicable):


- A. Failure to comply with this Directive will result in disciplinary action in accordance with the Municipal Civil Service Rules of the City of San Antonio, Rule XVII, Section 2. Discipline will be evaluated and based upon the number of violations and severity of the incident. The Human Resources Department must be consulted by a department when assessing the appropriate level of disciplinary action.
- B. Employees who fail to follow and administer this Directive will be disciplined under the authority of the Department Director.
- C. This Administrative Directive does not supersede the Department Director's authority over the determination of final disciplinary actions taken, particularly in cases where the safety of the general public or City employees are significantly compromised by an infraction of this administrative Directive. A Department Director may choose to assess more severe disciplinary action against an employee depending on the severity of the infraction.

ADMINISTRATIVE DIRECTIVE 7.5 Acceptable Use of Information Technology

Effective Date: December 1, 2005

Revision Date(s):

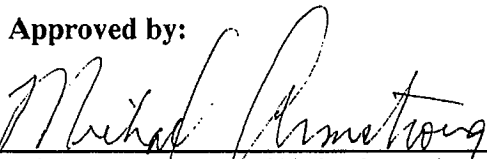
This Directive supersedes all previous correspondence on this subject. Information and/or clarification may be obtained by contacting the ITSD Department at 207-8301.



Hugh Miller, Jr., Interim Director ITSD

11/15/05
Date

Approved by:



Michael Armstrong, Chief Information Officer

11-15-05
Date

Approved by:



Sheryl Sculley, City Manager

11-15-05
Date

ADMINISTRATIVE DIRECTIVE 7.6

Security and Passwords

Effective Date: November 30, 2005

Revision Date(s):

I. PURPOSE:

This Administrative Directive establishes a general framework for securing the electronic assets of the City, and provides guidance for specific security issues that have general application in the City's technology environment. This directive supports and supplements Administrative Directive 7.5 – Acceptable Use of Information Technology. Nothing in this directive supersedes provisions of Directive 7.5.

II. POLICY:

- A. The City's computing and technology environment, along with the data it creates and maintains is a valuable asset. The City will take all reasonable and necessary measures to maintain the availability, dependability and integrity of that environment. The City will analyze risks carefully to maintain a proper balance between security measures and the requirement that its technology environment effectively and efficiently support its operations.
- B. The Information Technology Services Department has primary responsibility for security of the City's electronic systems, and may establish such policies, procedures and standards as may be necessary to assure the security of City systems. ITSD shall develop and maintain a comprehensive security program for the City, and shall provide guidance and advice to technology users in maintaining appropriate security.
- C. All technology users are responsible for following security policies and guidelines, and shall participate in developing those policies and guidelines when requested to do so.
- D. Passwords are an important element of computer security. A poorly chosen password may result in the compromise of the City's network. All City employees (including contractors and vendors with access to City systems) are responsible for taking appropriate steps to select and secure passwords. **Any activity performed under a user-id/password combination is presumed to have been performed by that user and is the responsibility of that user.**
- E. ITSD shall establish policies that address password use for Administrative User Accounts, Service Accounts and System-level Accounts.

III. DEFINITIONS:

- A. **Administrative User Account:** Any individually assigned user account that is used to perform technology related administrative functions or used in activities dealing with sensitive data (e.g. user management, network management, Oracle database administrator, SAP administrator).
- B. **Service Account:** Any account that is used for the operation or delivery of a technology service through an automated system.

ADMINISTRATIVE DIRECTIVE 7.6

Security and Passwords

Effective Date: November 30, 2005

Revision Date(s):

- C. System-level Account: Any account that is necessary for the operation of a technology system (e.g., root, database administration accounts, NT admin, application administration accounts, etc.).
- D. User-level Account: Any assigned non-administrative user account (e.g., email, web, desktop computer, etc.)

IV. POLICY GUIDELINES:

This directive applies to all Technology Users who access the City's networks and any data and applications that reside on those networks.

V. RESPONSIBILITIES:

Information Technology Services Department

- A. Organizational responsibility for the development, implementation, maintenance, and compliance monitoring of this directive is placed with ITSD.
- B. ITSD will provide City departments with initial communication and training regarding this Directive. However, City Department Directors are ultimately responsible for communicating the policies and standards established in this directive to all personnel in their respective departments and for ensuring compliance within their respective departments with those policies and standards.
- C. ITSD is responsible for communicating the policies and standards established in this directive to all third-party users and for ensuring their compliance. Those City departments who work with the third-party users are responsible for identifying the third-party users to ITSD.
- D. ITSD reserves the right to terminate services to any user found in breach of this directive and if continued connectivity provides a threat to the City or City-administered technology or equipment. ITSD will attempt to contact the user's DSS prior to disconnecting the service as long as such notification does not allow further degradation of the City-administered technology or equipment. Such notification will be made after the disconnection if prior coordination was not possible.

Department Directors and their designees

- A. Supervisors shall ensure that employees and any affected third-party users (contractors, consultants, agencies having a contractual relationship with the City, part-time and temporary employees) have received a copy of this directive.
- B. Department Directors should ensure that no departmental personnel, including administrative staff, request access to or maintain lists or databases of other user's passwords.
- C. Department Directors are responsible for any disciplinary action taken against employees who violate this directive in accordance with paragraph VII. The Human

ADMINISTRATIVE DIRECTIVE 7.6

Security and Passwords

Effective Date: November 30, 2005

Revision Date(s):

Resources Department will provide guidance as required to City departments regarding appropriate disciplinary action to be taken against employees who violate this policy.

Employees

- A. Employees are accountable for the proper use of City-owned technology, and should be aware that they are responsible for any information that they generate or distribute through the City's technology systems. Any activity performed on a workstation under an employee's login ID is presumed to be performed by that employee.
- B. Employees are responsible for complying with this directive, and with security policies and processes that may be developed by ITSD.
- C. Employees shall take reasonable and necessary care to prevent unauthorized access to workstations, laptops and other portable devices.
- D. Employees shall report any suspected security violation or threat to the ITSD Help Desk immediately.

Human Resources Department

- A. Human Resources will provide guidance to departments for disciplinary actions associated with violations of this directive.

VI. PROCEDURES:

- A. ITSD recommends the use of "strong" passwords. Strong passwords:
 - 1. Contain characters from three of the following four categories:
 - a) English uppercase characters (A through Z)
 - b) English lowercase characters (a through z)
 - c) Base 10 digits (0 through 9)
 - d) Non-alphanumeric characters (e.g., !, \$, #, %)
 - 2. Are at least 8 alphanumeric characters long.
 - 3. Are not words in any language, slang, dialect, or jargon.
 - 4. Are not based on personal information, such as the names of family.
 - 5. Are not common usage word such as:
 - a) Names of family, pets, friends, co-workers, fantasy characters, etc.
 - b) Computer terms and names, commands, sites, companies, hardware, software.
 - c) The words "COSA", "sananton" or any derivation.
 - d) Birthdays and other personal information such as addresses and phone numbers.
 - e) Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
 - f) Any of the above spelled backwards.

ADMINISTRATIVE DIRECTIVE 7.6

Security and Passwords

Effective Date: November 30, 2005

Revision Date(s):

- g) Any of the above preceded or followed by a digit (e.g., secret1, 1secret)
- B. All user passwords will expire at intervals of ninety (90) days. Users will be prompted to change passwords beginning 10 days before the next expiration date.
- C. Passwords may not be re-used.
- D. Accounts will be "locked" after three (3) unsuccessful attempts to logon using a password. Users whose accounts have been locked must call the ITSD Help Desk to reset the user's password.
- E. Password Protection Guidelines for Users:
 - 1. Do not write passwords down, store them on-line, or reveal them in electronic communication.
 - 2. Do not use the same password for COSA accounts as for other accounts.
 - 3. Do not share COSA passwords with anyone. Passwords should be treated as sensitive, confidential COSA information.
 - 4. ITSD support personnel may require a user's password to resolve a problem. ITSD prefers that the user be present to enter a required password. If a password must be revealed to the technician, ITSD suggests that the password be changed as soon as is practicable.
 - 5. Do not talk about a password in the presence of others.
 - 6. Do not hint at the format of a password (e.g., "my family name").
 - 7. Do not reveal a password on questionnaires or security forms.
 - 8. Do not use the "Remember Password" feature of applications (e.g., websites, Outlook, and Netscape Messenger).
 - 9. Do not store passwords in a file on ANY computer system (including Palm Pilots or similar devices) without encryption.
- F. If anyone other than ITSD support personnel requests a password from an employee, refer that person to the Information Technology Services Department to establish access to COSA systems and files as needed.
- G. ITSD is the only authorized password reset agent. ITSD support personnel may request information required to verify a user's identity.
- H. If an account or password is suspected to have been compromised, report the incident to ITSD and change all passwords.
- I. System, service, and other non-changeable passwords will be assigned and cataloged by ITSD. ITSD will take reasonable and necessary precautions to protect these passwords from compromise.

ADMINISTRATIVE DIRECTIVE 7.6

Security and Passwords

Effective Date: November 30, 2005

Revision Date(s):

VII. DISCIPLINE

- A. Failure to comply with this directive will result in disciplinary action in accordance with the Municipal Civil Service Rules of the City of San Antonio, Rule XVII, Section 2. Discipline will be evaluated and based upon the number of violations and severity of the incident. The Human Resources Department must be consulted by a department when assessing the appropriate level of disciplinary action.
- B. Employees who fail to follow and administer this directive will be disciplined under the authority of the Department Director.
- C. This Administrative directive does not supersede the Department Director's authority over the determination of final disciplinary actions taken, particularly in cases where the safety of the general public or City employees are significantly compromised by an infraction of this administrative Directive. A Department Director may choose to assess more severe disciplinary action against an employee depending on the severity of the infraction.

This directive supersedes all previous correspondence on this subject. Information and/or clarification may be obtained by contacting the ITSD Department at 207-8301.




Hugh Miller, Jr., Interim Director ITSD

11/29/05

Date

Approved by:



Michael Armstrong, Chief Information Officer

11/29/05

Date

Approved by:



Sheryl Sculley, City Manager

11-29-05

Date

Exhibit D: UHS Benefits Summary

UHS Summary of Benefits

Medical

University Health System offers two medical plan options administered by Community First Health Plans.

- University Family Care Plan
- University Family Care Plus Plan

Coverage Category	Family Care Plan	Family Care Plus Plan
Employee	\$35.45/month	\$251.69/month
Employee & spouse	\$61.97/month	\$583.42/month
Employee & child(ren)	\$60.99/month	\$656.07/month
Employee & family	\$89.60/month	\$914.93/month

Dental

University Health System Self-Insured Dental Plan - Benefit Planners, Inc.

- The University Health System dental plan is a traditional PPO no co-payment plan that allows employees the freedom to see any dentist nationwide. BPI offers the DenteMax Provider Network with over 30,000 locations across the country.
- If \$300 or more worth of dental services are required, the dentist will need to submit a pre-determination of benefits form to Benefit Planners, Inc. for approval.
- If a DenteMax provider is selected, the employee will pay up to 35% less in out-of-pocket expenses than if an out-of-the-network dentist is used.

CIGNA Dental Plan

- The second dental option is CIGNA Dental Plan, a managed dental care DMO plan. CIGNA allows employees to select a general dentist from the provider network. The primary general dentist then refers employees to a specialist for extended care. This plan covers preventive care; restorative care; periodontics; adult and child orthodontics without deductibles, co-insurance or maximums.

Coverage Category	Benefit Planners	CIGNA
Employee	\$10.37/month	No Cost
Employee & spouse	\$30.87/month	\$11.36/month
Employee & child(ren)	\$41.62/month	\$15.41/month
Employee & family	\$54.36/month	\$20.21/month

Life

Group Term Life

- University Health System provides Group Term Life Insurance to all regular full-time and part-time employees (24+ standard hours) at no cost.
- Group Term Life Insurance covers employees on or off the job. Dependents are not covered under this policy. The amount of Group Term Life coverage is \$4,000, subject to applicable age reductions for eligible employees age 70 and over according to the schedule in the policy.

Supplemental Life Insurance

- University Health System offers eligible employees the option of purchasing additional low-cost life insurance coverage that can be adjusted to meet specific individual needs. Employees may purchase supplemental life and accidental death and dismemberment coverage in an amount equal to 1 or 2 times their annual rate of basic earnings minus \$4,000. If an employee should become disabled prior to age 60, premiums for life insurance can be waived after a six-month disability.

Accidental Death and Dismemberment

- University Health System provides Accidental Death and Dismemberment (AD&D) Insurance to all regular full-time and part-time employees (24+ standard hours) at no cost.
- AD&D Insurance covers employees on or off the job. Dependents are not covered under this policy. The amount of each employee's AD&D coverage is \$4,000, subject to applicable age reductions for eligible employees age 70 and over according to the schedule in the policy. The AD&D benefit is also determined by the extent of the accidental loss.

Dependent Group Life

- Life insurance coverage is available for employees to purchase for their spouse and/or child(ren) who are up to the age of 25 and maintain full-time student status.
- Employees pay one premium no matter how many eligible dependents they cover.

Dependent Group Life Premiums	
Premium	\$2.60/month
Spouse	\$10,000 in coverage
Child	\$5,000 in coverage

Universal Life Insurance

- University Health System offers Universal Life Insurance at competitive rates according to the benefit chosen. Universal Life insurance offers an easy and affordable way to safeguard the family's future by providing death benefits.
- Once enrolled, the plan is theirs even if they separate from service or have a change in health. The employee's insurance premiums are then directly billed to their home. The insurance coverage and premium remains the same unless the employee chooses to adjust them.
- The plan also offers an accelerated death benefit to provide employees and their dependents with living benefit choices for the future.
- This plan builds cash value over time when employees continue to pay premiums. Employees can withdraw cash or borrow against their policy's accumulated cash value for financial emergencies, investment opportunities or other needs (subject to applicable surrender charges).

Disability

Short-Term Disability Insurance

- Short-Term Disability can provide employees with an income in case they experience a non-work related illness or injury. Short-Term Disability provides income to help continue living expenses such as rent, food, utilities, car payments, etc. University Health System offers all eligible full-time and part-time employees (20 hours or greater) with this extremely valuable opportunity to purchase protection at a low cost.
- Short-Term Disability benefits begin on the 31st day of disability due to continuous disability. During the waiting period, employees will use their Paid Time Off days.
- Employees can select a weekly benefit equal to, or less than, the one listed for their salary range up to \$1,400 per week. This benefit provides up to 22 weeks of pay continuation. If employees enroll at the time of hire and are selecting a weekly benefit of \$700 a week or less, there is no evidence of insurability requirement. Employees will be required to provide evidence of insurability if they are electing coverage of \$700 a week or more or are enrolling after the first 30 days of employment. If disability continues beyond the maximum benefit period, Long-Term Disability (LTD) benefits may continue to provide the employee with income protection if the employee is eligible for LTD at the time of disability.

Long-Term Disability Insurance

- University Health System provides this very valuable benefit at no cost to all eligible full-time and regular part-time employees (32 hours or greater) after one year of continuous regular employment. Long-Term Disability (LTD) coverage provides partial income protection for the eligible employee in the event of long-term disability.
- Eligibility begins after six months of being disabled and benefits are paid once the claim has been approved.
- Total benefit paid is 60 percent of monthly earnings up to \$6,000 per month [the total payable benefit will be offset by other sources of income (e.g. Social Security, Disability, etc.)].

- Length of benefit will depend upon disability and/or age of participant when disability begins.

Cancer, Dread Disease, ICU Policy

- University Health System offers a Cancer, Dread Disease, ICU Policy. This policy pays cash benefits directly to employees, regardless of other coverage, for cost typically not covered under their insurance policy such as:
- Missed work days for a covered family member's treatment; transportation for non-local treatment; meals required away from home; motels during non-local treatment; babysitting for children at home; long distance phone calls; loss of wages while caring for a covered family member; and parking/hotel fees.
- The plan also includes an intensive care/coronary care component. When a covered person is confined to an intensive care unit, the plan will pay \$300 to 600 per day up to a pre-determined limit per confinement as a result of any sickness or accident.
- Once enrolled, the participant remains on the plan even if he/she is separated from service or has a change in health.
- Insurance premiums are then directly billed to the participant's home. The insurance coverage and premium remain the same.

Cancer Dread Disease, ICU Policy (Bi-weekly Rate)	Basic	Enhanced
Individual	\$7.36	\$10.11
Family	\$12.75	\$17.64

Group Accident Hospital Income Plan

- All regular full-time employees who have completed one year of service are automatically covered by this plan. There is no annual premium and the plan pays \$100 per day if the employee is hospitalized in the event of a non work-related accident. Admission must be in a hospital, not a skilled nursing facility.
- Covers up to 180 days annually
- A \$500,000 lifetime maximum
- Coverage for employees only

FSA

Flexible Spending Accounts

- University Health System provides an opportunity to participate in two types of flexible spending accounts (FSAs) — a Health Care FSA and a Dependent Care FSA. Employees may elect to participate in one or both of these accounts. The accounts allow employees to set aside money on a pre-tax basis to reimburse for eligible health and dependent care expenses. Employees save money by not paying taxes on the amount set aside. Employees must re-elect this coverage every year during annual enrollment. Coverage is not automatic and will not roll over from year to year.

The Health Care Reimbursement Account

- The Health Care Reimbursement Account exists to help employees pay for healthcare expenses that are medically necessary, non-cosmetic in nature and not fully covered under their medical or dental plan. The maximum amount each employee can deposit into this account in 2007 is \$5,000.

Dependent Care Reimbursement Account

- The Dependent Care Reimbursement Account exists to help employees pay for dependent care expenses for their children under age 13 or adult family members who are disabled and depend on the employee for support. If dependent care is required to enable the employee (or a spouse or single person) to work, these expenses may be eligible for reimbursement. Included are payments to child care centers, nursery schools, kindergarten and schools for children up to but not including first grade. Eligible expenses also include payment for summer day camps, after school care and elder care. Care within the employee's home by a relative, or a non-relative, as long as such person is reporting payments as income, is also eligible. The maximum amount each employee can deposit in 2007 is \$5,000, or \$2,500 if the employee is married, but filing

separately.

Retirement

Pension Plan

- A contribution equal to 2% of gross pay is mandatory upon achievement of eligibility and thereafter until the time of retirement or separation from employment with University Health System. The cost of plan participation will be automatically deducted from each bi-weekly paycheck on a pre-tax basis. University Health System contributes the majority of funding for this pension plan. Then University Health System makes its contributions directly to the Pension Trust each year.
- Employees are eligible to begin participating in the Plan on the next January 1st or July 1st following attainment of 21 years of age and 1 year of continuous service with the Health System during which the employee worked at least 1000 hours.
- Participation is automatic upon attainment of the eligibility criteria. University Health System believes that a retirement income is essential for all employees. For this reason, if an employee is eligible to participate in the Plan, participation is required as a condition of employment.
- Vesting status entitles employees to a pension benefit that may commence at age 55 or later, as elected. If an employee should terminate from the Health System, but is vested, he/she will be entitled to draw the pension benefit at age 55 or later, as elected.
- For the purpose of vesting, employees will be credited with one year of vesting service for each year of continuous service in which 1000 or more hours are worked. Employees will become vested in the Plan upon completion of five years of vesting service. Employees are 100% vested once they have accrued five years of vesting service.
- If employees separate from employment before being vested, they are not eligible for a pension benefit, but their contributions to the Plan will be refunded with interest at the annual rate of 4 ½ percent.

457 Deferred Compensation Plan

- Deferred Compensation Plans provide a way for employees to build their retirement savings on a pre-tax basis through payroll deduction. "Deferred Compensation" means that a certain portion of current earnings are set aside without being taxed and are invested in investment vehicles where money grows on a tax-deferred basis until the employee retires or separates from the Health System. The program allows all employees of the Health System to participate in a savings program that provides considerable savings from an income tax standpoint, as authorized by the Internal Revenue Service. Employees may begin deferring compensation into their accounts at any time and may defer as much as they wish, up to current annual limits established by law (up to \$15,500.00 in 2007).
- Beginning with the year in which employees reach age 50, they may make additional contributions. Also, for each one of their last three taxable years prior to age 65, employees may make additional contributions, if maximum allowable contributions in prior years were not made.
- Employee catch-up contributions may not exceed the amount they could have contributed in prior years but did not. No employer match is provided on catch-up contributions.
- There are no vesting requirements for the 457 Deferred Compensation Plan. Employees are always vested in their own contributions and interest. Participation in the Health System's Deferred Compensation Plan is voluntary.
- University Health System will match employee contributions, up to 4% of their pay, to a 457 Retirement Savings Account, at the rate of 25% (\$0.25 on the \$1).
- Employees become eligible for the University Health System Match Savings Plan on the next January or July 1st following attainment of 21 years of age and 1 year of continuous service with the Health System, during which 1000 hours are worked.
- The vesting requirement for the Match Savings Plan is the same as the vesting requirements for the University Health System Pension Plan. Employees are 100% vested once they have accrued five years of vesting service. If an employee leaves the Health System before being vested in the Match Savings Plan, they will forfeit the matching contributions made by the Health System to their match account and any return on those contributions.

Summary

Retirement Plans Summary		
Plan	Enrollment	Deduction Amount
Pension	Automatic	2% of gross pay
457 Deferred Compensation	Voluntary	1-100% of gross pay, but no more than \$15,500
Match Savings Plan	Automatic	UHS Contributions

Other Benefits

Employee Assistance Program (EAP)

- The Choice CARE Employee Assistance Program is a completely free and confidential counseling and support service for Health System employees and their families. Choice CARE counselors will provide counseling at no cost to all regular full-time and part-time employees, their spouse and dependent children under the age of 21 living at home. Each family member is entitled to eight sessions per problem, per year for marital, family, behavioral, substance abuse, grief, depression and other forms of counseling support.

Educational Benefits

- Tuition reimbursement (up to \$1500 annually)
- Continuing education and certification reimbursement (up to \$200 per year)
- Free on-site classes for University Health System employees
- Contact hours for nursing staff

Paid Time Off (PTO)

- In recognition of our unique individual needs, the Health System offers a Paid Time Off (PTO) program that allows each employee to accumulate and schedule time off according to individual needs. Eligible employees begin accruing PTO benefit hours in their own personal bank from the first day of work. When we need time off for vacations, holidays, illnesses, injuries, personal business, school conferences, or any other reason, we draw from our bank of PTO time. Unused PTO remains in the bank for future use and can accumulate up to 1,040 hours.
- Some employees choose to sell their PTO time to help fund school, holiday, vacation and other expenses. Once employees have accrued 256 hours of PTO, they can cash part of it in for 50 percent of its current value. The sell-back option is available every pay period.

	PTO Accrual Rates	Accrual per pay period	Per Year	Maximum
Full-time	1st Year	8.62	28 days	1040 Hours
	2nd Year	8.93	29 days	1040 Hours
	3rd Year	9.24	30 days	1040 Hours
	4th Year	9.54	31 days	1040 Hours
	5th Year	9.85	32 days	1040 Hours
	6th Year	10.16	33 days	1040 Hours
	7th Year	10.47	34 days	1040 Hours
	8th Year	10.77	35 days	1040 Hours
	9th Year	11.08	36 days	1040 Hours
	10th Year	11.39	37 days	1040 Hours
	11+ Years	11.7	38 days	1040 Hours
Part-time	16-39 hrs	0.1077	24 hrs=16.80 days	36-39 hrs =28 days

Exhibit E: Positions and Other Expense Items

Positions Transitioning to UHS				
	Full-time		Part-time	
Position	GF	Grant	Grant	Total
Accountant II		1		1
Administrative Assistant I		2		2
Building Custodian	7			7
Case Aide	2	1		3
Custodial Services Crew Leader	1			1
Dept Systems Specialist		1		1
Health Program Specialist	1			1
LVN	13			13
Nursing Program Manager	1			1
Administrative Associate	14	3		17
PH Nurse	14	1		15
PH Nurse Practitioner	5	1	1	7
PH Nurse Supervisor	8	1		9
Public Health Aide	21	6	1	28
Sr. Administrative Assistant	1			1
Sr. Office Assistant	1			1
Sr. PH Nurse	8	4		12
PH Physician	1		4	5
Total	98	21	6	125

SAMHD/UHS Calculation of Costs for Transition of Clinical Preventive Health Services			
Item	11 Month Estimate	8 Months - FY 2008 Estimate	3 Months - FY 2009 Estimate
<i>Estimated General Fund Costs for Services</i>	\$4,801,876	\$3,424,204	\$1,377,672

Budgeted General Fund Revenues			
HMO Medicaid Reimbursement	\$370,433	\$256,854	\$113,579
Medicaid/Medicare	\$89,424	\$66,748	\$22,676
Patient Co-pay	\$139,149	\$92,361	\$46,788
<i>Total Budgeted General Fund Revenues</i>	<i>\$599,006</i>	<i>\$415,963</i>	<i>\$183,043</i>
UHS Contract Amount (less revenues)¹	\$4,202,870	\$3,008,241	\$1,194,629

Budget Detail			
General Fund Personal Services and Other Items	Current COSA Proposal Amount	8 Month Payment	3 Month Payment
General Fund Salaries (w/ half internal equity)	\$3,283,031	\$2,387,659	\$895,372
Social Security (7.65%)	\$259,464	\$188,701	\$70,763
Health Benefits (COSA \$8,280/FT employee) / UHS	\$290,672	\$211,398	\$79,274
<i>Personal Services Subtotal</i>	<i>\$3,833,167</i>	<i>\$2,787,758</i>	<i>\$1,045,409</i>

OPEB	\$45,472	\$45,472	\$0
MD Incentive	\$9,167	\$6,667	\$2,500
Annual Leave Payout ¹	\$178,973	\$178,973	\$0
Increased Annual Leave (UHS Internal Equity)	\$26,660	\$26,660	\$0
Workers/Unemployment Compensation	\$50,902	\$37,020	\$13,882
Base PTO Accrual Rate (FY 08 Amount)	\$36,647	\$36,647	\$0
Base PTO Accrual Rate (FY 09 Amount)	\$192,520	\$0	\$192,520
Additional PTO Accrual Rate (Based on City Years of Service)	\$91,667	\$66,667	\$25,000
UHS Pension	\$183,260	\$133,280	\$49,980
<i>Other Items Subtotal</i>	<i>\$815,268</i>	<i>\$531,386</i>	<i>\$283,882</i>
<i>Other Non-Position-Related Items Subtotal</i>	<i>\$153,441</i>	<i>\$105,060</i>	<i>\$48,381</i>
Estimated General Fund Costs for Services	\$4,801,876	\$3,424,204	\$1,377,672

Estimated Grant Balances to be Transferred to UHS			
	Ending Date of Grant Contract	Total Grant Award (without program income)	Estimated Grant Balance on 1/31/07
Breast & Cervical Cancer Screening Project	6/30/2008	\$200,200.00	\$126,000.00
Refugee Resettlement	8/31/2008	\$143,495.00	\$95,640.00
Title V Family Planning	8/31/2008	\$129,649.00	\$60,000.00
Title V Maternal and Child Health	8/31/2008	\$212,998.00	\$130,000.00
Title X ²	8/31/2008	\$39,882.00	\$32,700.00
Title X Male Involvement ¹	8/31/2008	\$125,000.00	\$72,917.00
Title XX Family Planning	8/31/2008	\$357,628.00	\$177,400.00
UTHSCSA Patient Navigator	8/31/2008	\$148,194.00	\$86,700.00
Totals		\$1,357,046.00	\$781,357.00

¹ This amount will be reduced by any payment for accrued annual leave made directly to transitioning staff prior to employment with UHS (if any).

² Does not include \$86,913 that will be subcontracted to SAMHD for the Male Health Grant

Exhibit F: Summary of SAMHD Grants for Services Transitioning to UHS

Grants Transitioning to UHS				
Grant/ Contract	Funder	Services Provided	End of Current Grant Cycle	Award for Current Grant Cycle
Breast & Cervical Cancer Control Services	DSHS	Fee for service grant to support early detection of breast and cervical cancer through outreach and screening.	6/30/2008	\$200,200
Title V Maternal & Child Health	DSHS	Fee for service grant provides services to pregnant women who are without third party funding at the time of care.	8/31/2008	\$212,998
Title V Family Planning	DSHS	Fee for service grant supports services to women of child bearing age (18-44) who are ineligible for Title XIX for annual exams and family planning services.	8/31/2008	\$129,649
Title X Family Planning	DSHS	Supports services in conjunction with Title XX and Title XIX. Title X provides infrastructure building support. Confidential teen services are provided under Title X objectives. Includes both clinical and population-based components.	8/31/2008	\$39,882
Title X Male Health	DSHS	Clinical and population based services to address reproductive health for males 15-25 years of age. Residual funds for FY 08 will be contracted back to SAMHD.	8/31/2008	\$125,000
Title XX Family Planning	DSHS	Fee for service grant provides services to women of child bearing age (18-44) who are ineligible for Title XIX.	8/31/2008	\$357,628
Refugee Resettlement	DSHS	Fee for service grant supports social (through subcontract) and medical services to families who are part of the U.S. Immigration Services Program including communicable disease screening, treatment of preexisting diseases, and identifying a medical home.	9/30/2008	\$143,495
Patient Navigator	UTHSCSA	Assists Hispanic women with abnormal findings or diagnoses related to breast and cervical cancer to find follow up care.	8/30/08	\$148,194